(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年7 月24 日 (24.07.2003)

PCT

(10) 国際公開番号
WO 03/061189 A1

(51) 国際特許分類[7]: H04L 9/08, 9/32, G06F 12/14, 15/00, 13/00

(21) 国際出願番号: PCT/JP03/00107

(22) 国際出願日: 2003 年1 月9 日 (09.01.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-7656 2002 年1 月16 日 (16.01.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 瀧 隆太 (TAKI,Ryuta) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 宮田 正昭, 外(MIYATA,Masaaki et al.); 〒104-0041 東京都 中央区 新富一丁目１番７号 銀座ティーケイビル６階 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

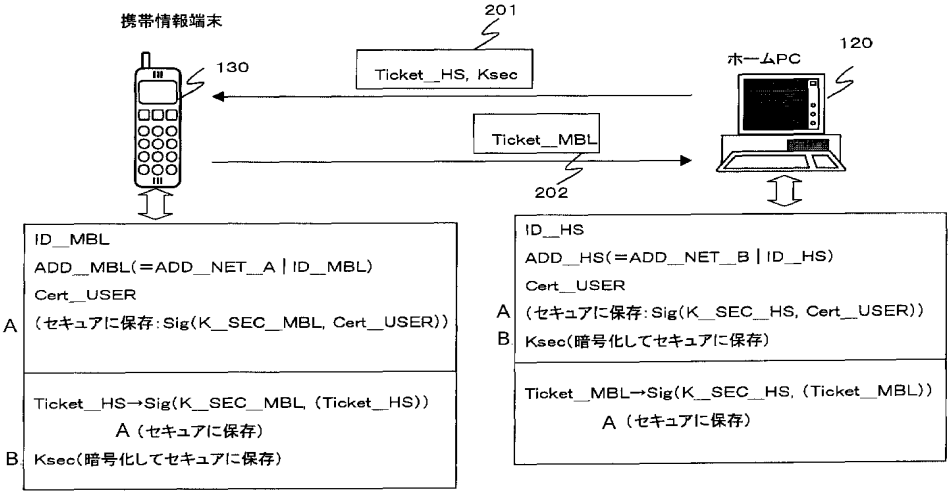
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: CONTENT DELIVERY SYSTEM

(54) 発明の名称: コンテンツ配信システム



130...MOBILE INFORMATION TERMINAL
120...HOME PC

A...STORE SECURELY
B...ENCRYPT AND STORE SECURELY

(57) Abstract: A system is realized that allows a secure processing even when an apparatus that requests a download is not the terminal apparatus that is the destination of the download. A content delivery server receives the signature ticket of a download designation from a content download requesting terminal, and verifies the ticket to confirm that the apparatus of the download destination is an apparatus approved by the download requesting terminal, thereby confirming the correctness of the device of the download destination without establishing a direct authentication therewith. A content signature key (Ksig) or hash value is transmitted/received as data that can be cryptographic-processed only at the download requesting and destination apparatuses, and a tampering check of the contents and the like can be executed only at the correct download destination apparatus.

[続葉有]

WO 03/061189 A1

(57) 要約:

ダウンロード要求とダウンロード先端末を異なる装置とした場合のセキュアな処理を可能としたシステムを実現する。コンテンツ配信サーバは、コンテンツダウンロード要求端末からダウンロード先の署名チケットを受信して、チケットを検証してダウンロード先の装置が、ダウンロード要求端末の承認した装置であることを確認して、ダウンロード先機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認を行なう。また、コンテンツ署名用鍵［Ｋｓｉｇ］またはハッシュ値を、ダウンロード要求および先の装置においてのみ暗号処理可能なデータとして送受信し、コンテンツの改竄チェック等を正当なダウンロード先装置においてのみ実行可能とした。

明　細　書

コンテンツ配信システム

技術分野

本発明は、コンテンツ配信システム、コンテンツ配信方法、および情報処理装置、並びにコンピュータ・プログラムに関し、特に、コンテンツのユーザ機器に対する送信、ダウンロード処理をセキュアに実行し、かつ利便性を高めたコンテンツ配信システム、コンテンツ配信方法、および情報処理装置、並びにコンピュータ・プログラムに関する。

背景技術

昨今、画像データ、音声データ、ゲームプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワークを介してデータ配信サーバからユーザの機器、例えばＰＣ、あるいは携帯機器としてのモバイルコンピュータ、ＰＤＡ、携帯電話等に送信し、各機器の記憶媒体にデータをダウンロードするといった携帯でのコンテンツの利用が広く普及してきている。

ＰＣ、携帯端末等の情報機器には、コンテンツをネットワークから受信するためのインタフェースを有し、さらにコンテンツの再生に必要となる制御手段、プログラム、データのメモリ領域として使用されるＲＡＭ、ＲＯＭ等を有する。

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、インターネット等を介してユーザ機器内のハードディスク、フラッシュメモリ等の記憶媒体に格納され、コンテンツ再生機器として利用されるＰＣ、携帯端末等の情報機器に対するユーザ指示により記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

コンテンツ配布、すなわち、コンテンツ配信サーバからユーザ機器に対するコンテンツのダウンロード実行に際しては、ユーザ機器が正当なコンテンツ利用許

可を得られたものであるかの認証、例えば公開鍵暗号方式、あるいは共通鍵暗号方式等の各種の認証処理を行なって、ユーザ機器の正当性を確認する処理が行なわれることが多い。

昨今の様々な情報処理端末の普及に伴い、個人ユーザであっても自宅にはＰＣを有し、屋外では、携帯電話、モバイルコンピュータ、ＰＤＡ等の携帯機器を使用するといったように、複数の情報機器の利用が一般的になっており、このような各種の機器から、コンテンツ配信サーバに対して様々なコンテンツのダウンロードを要求することが可能になっている。

認証を条件としたコンテンツ・ダウンロードが実行される場合、例えば、ユーザが屋外において携帯端末を利用している際に、コンテンツ配信サーバに対して、コンテンツの配信を要求すると、ユーザの利用中の携帯端末とサーバ間の認証が実行され、携帯端末が正当である場合にコンテンツが送信される。また、ユーザが屋内においてＰＣを利用している際に、コンテンツ配信サーバに対して、コンテンツの配信を要求すると、ユーザの利用中のＰＣとサーバ間の認証が実行され、ＰＣが正当である場合にコンテンツが送信され、ダウンロードが可能になる。すなわち、コンテンツ配信サーバは、コンテンツのダウンロード先の機器との認証を行なって、ダウンロードの許可を行なうことになる。

ダウンロード対象となるコンテンツは多様化しており、携帯電話等の小メモリに格納可能な小容量の例えばミュージックコンテンツ、ゲームプログラム等がある一方、ＰＣ等のハードディスクには格納可能であるが、携帯電話等の小メモリには格納不可能な大容量の例えば映画等の動画像コンテンツ等などもダウンロード対象コンテンツとして流通している。

ユーザがフラッシュメモリ等の比較的小容量のメモリを有する携帯端末を利用しているときに、大容量の映画等のコンテンツのダウンロードをコンテンツ配信サーバに要求しても、携帯端末のメモリには格納不可能であり、ダウンロード処理をあきらめざる得ないのが現状である。

発明の開示

本発明は、上述の問題点に鑑みてなされたものであり、ＰＣ、携帯端末等、複

数のデータ受信可能な情報処理装置を有するユーザが、いずれか１つのの機器、例えば携帯端末からコンテンツ配信サーバにアクセスし、ユーザの所有する他の機器、例えばＰＣに対するコンテンツ配信サーバからのコンテンツ送信、およびダウンロード処理をセキュアに実行可能としたコンテンツ配信システム、コンテンツ配信方法、および情報処理装置、並びにコンピュータ・プログラムを提供することを目的とする。

本発明の第１の側面は、

自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行する第１の情報処理装置と、

コンテンツのダウンロード先として指定される第２の情報処理装置と、

前記第１の情報処理装置からのコンテンツダウンロード要求を受信して、前記第２の情報処理装置に対するコンテンツの送信処理を実行するコンテンツ配信サーバとを有し、

前記第１の情報処理装置は、

前記第２の情報処理装置の電子署名がなされたチケットを前記コンテンツ配信サーバに送信する処理を実行し、

前記コンテンツ配信サーバは、

前記チケットの電子署名の検証を実行し、該検証に成功したことを条件として、前記第２の情報処理装置が前記第１の情報処理装置の承認したコンテンツダウンロード先であると判定して、前記第２の情報処理装置に対するコンテンツ送信を実行する構成を有することを特徴とするコンテンツ配信システムにある。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記第１の情報処理装置と、前記第２の情報処理装置は、共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有し、前記第１の情報処理装置は、前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、前記第２の情報処理装置は、前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］による暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］

の復号により取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行する構成であることを特徴とする。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記第１の情報処理装置と、前記第２の情報処理装置は、共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有し、前記第１の情報処理装置は、前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、前記第２の情報処理装置は、前記ホームネットエリア共有秘密鍵[Ｋｓｅｃ]による暗号化ハッシュ値[Ｅ(Ｋｓｅｃ,Ｈ(Ｍ))]の復号により取得したコンテンツのハッシュ値［Ｈ（Ｍ）］を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行する構成であることを特徴とする。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記第１の情報処理装置と、前記第２の情報処理装置は、それぞれ公開鍵暗号方式の公開鍵、秘密鍵を有し、前記第１の情報処理装置は、該第１の情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｋｓｉｇ）］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、前記第２の情報処理装置は、前記第１の情報処理装置の公開鍵[Ｋ＿ＰＵＢ＿ＭＢＬ]による暗号化鍵データ[Ｅ(Ｋ＿ＳＥＣ＿ＭＢＬ,Ｋｓｉｇ)]の復号により取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行する構成であることを特徴とする。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記第１の情報処理装置と、前記第２の情報処理装置は、それぞれ公開鍵暗号方式の公開鍵、秘密鍵を有し、前記第１の情報処理装置は、該第１の情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテン

ツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、前記第２の情報処理装置は、前記第１の情報処理装置の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］による暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］の復号により取得したコンテンツのハッシュ値［Ｈ（Ｍ）］を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行する構成であることを特徴とする。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記チケットは、前記第１の情報処理装置と、前記第２の情報処理装置各々の識別子（ＩＤ）を含むデータに対して、前記第２の情報処理装置の秘密鍵による電子署名がなされたチケットであり、前記コンテンツ配信サーバは、前記第２の情報処理装置の公開鍵を適用して、前記チケットの電子署名の検証を実行する構成であることを特徴とする。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記コンテンツ配信サーバは、前記チケットの電子署名の検証処理として、以下の処理（ａ）前記第２の情報処理装置の公開鍵証明書の署名（認証局署名）検証による公開鍵証明書の正当性確認処理、（ｂ）正当性の確認された公開鍵証明書からの前記第２の情報処理装置の公開鍵の取得処理、（ｃ）取得した前記第２の情報処理装置の公開鍵を適用した前記第２の情報処理装置のチケットの署名検証処理、の各処理を実行する構成であることを特徴とする。

さらに、本発明の第２の側面は、

自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行する第１の情報処理装置と、コンテンツのダウンロード先として指定される第２の情報処理装置と、前記第１の情報処理装置からのコンテンツダウンロード要求を受信して、前記第２の情報処理装置に対するコンテンツの送信処理を実行するコンテンツ配信サーバとを有するコンテンツ配信システムにおけるコンテンツ配信方法であり、

前記第１の情報処理装置において、

前記第２の情報処理装置の電子署名がなされたチケットを前記コンテンツ配信

サーバに送信するステップと、

前記コンテンツ配信サーバにおいて、

前記チケットの電子署名の検証を実行するステップと、

前記検証に成功したことを条件として、前記第２の情報処理装置が前記第１の情報処理装置の承認したコンテンツダウンロード先であると判定して、前記第２の情報処理装置に対するコンテンツ送信を実行するステップと、

を有することを特徴とするコンテンツ配信方法にある。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ配信方法において、前記第１の情報処理装置は、前記第１の情報処理装置と、前記第２の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、前記第２の情報処理装置は、前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］による暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］の復号により取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ配信方法において、前記第１の情報処理装置は、前記第１の情報処理装置と、前記第２の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、前記第２の情報処理装置は、前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］による暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］の復号により取得したコンテンツのハッシュ値［Ｈ（Ｍ）］を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ配信方法において、前記第１の情報処理装置は、該第１の情報処理装置の秘密鍵

［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｋｓｉｇ）］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、前記第２の情報処理装置は、前記第１の情報処理装置の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］による暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｋｓｉｇ）］の復号により取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ配信方法において、前記第１の情報処理装置は、該第１の情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、前記第２の情報処理装置は、前記第１の情報処理装置の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］による暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］の復号により取得したコンテンツのハッシュ値［Ｈ（Ｍ）］を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記チケットは、前記第１の情報処理装置と、前記第２の情報処理装置各々の識別子（ＩＤ）を含むデータに対して、前記第２の情報処理装置の秘密鍵による電子署名がなされたチケットであり、前記コンテンツ配信サーバは、前記第２の情報処理装置の公開鍵を適用して、前記チケットの電子署名の検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ配信サーバは、前記チケットの電子署名の検証処理として、（ａ）前記第２の情報処理装置の公開鍵証明書の署名（認証局署名）検証による公開鍵証明書の正当性確認処理、（ｂ）正当性の確認された公開鍵証明書からの前記第２の情報処理装置の公開鍵の取得処理、（ｃ）取得した前記第２の情報処理装置の公開鍵を適用した前記第２の情報処理装置のチケットの署名検証処理、の各処理を実行する

ことを特徴とする。

さらに、本発明の第３の側面は、

自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行する情報処理装置であり、

コンテンツのダウンロード先の第２の情報処理装置の電子署名がなされたチケットを格納した記憶手段と、

前記記憶手段に格納した前記チケットを含むコンテンツダウンロード要求コマンドを生成する制御手段と、

前記チケットを含むコンテンツダウンロード要求コマンドをコンテンツ配信サーバに対して送信する通信手段と、

を有することを特徴とする情報処理装置にある。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置の制御手段は、該情報処理装置と、前記第２の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を、前記第２の情報処理装置に対する送信データとして生成する構成を有することを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置の制御手段は、該情報処理装置と、前記第２の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を、前記第２の情報処理装置に対する送信データとして生成する構成を有することを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置の制御手段は、該情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｋｓｉｇ）］を、前記第２の情報処理装置に対する送信データとして生成する構成を有することを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置の制

御手段は、該情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］を、前記第２の情報処理装置に対する送信データとして生成する構成を有することを特徴とする。

さらに、本発明の第４の側面は、

自装置と異なるダウンロード先を指定したコンテンツダウンロード要求処理を実行するコンピュータ・プログラムであり、

コンテンツのダウンロード先の第２の情報処理装置の電子署名がなされたチケットを取得するステップと、

前記チケットを含むコンテンツダウンロード要求コマンドを生成するステップと、

前記チケットを含むコンテンツダウンロード要求コマンドをコンテンツ配信サーバに対して送信するステップと、

を有することを特徴とするコンピュータ・プログラムにある。

さらに、本発明の第５の側面は、

コンテンツの送信処理を実行するコンピュータ・プログラムであり、

第１の情報処理装置から自装置と異なるダウンロード先として第２の情報処理装置を指定したコンテンツダウンロード要求処理を受信するステップと、

前記コンテンツダウンロード要求に含まれるダウンロード先の第２の情報処理装置の電子署名がなされたチケットに含まれる電子署名検証処理を実行するステップと、

前記検証に成功したことを条件として、前記第２の情報処理装置に対するコンテンツ送信を実行するステップと、

を有することを特徴とするコンピュータ・プログラムにある。

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供すること

により、コンピュータ・システム上でプログラムに応じた処理が実現される。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

図面の簡単な説明

図１は、本発明のコンテンツ配信システムの概要を説明する図である。

図２は、本発明のコンテンツ配信システムにおけるホームネットエリアのデバイス構成、格納データ等ついて説明する図である。

図３は、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例１の処理シーケンスを説明する図である。

図４は、本発明のコンテンツ配信システムのコンテンツ配信処理例１におけるダウンロード要求装置である携帯情報端末の処理を説明するフローチャートを示す図である。

図５は、本発明のコンテンツ配信システムのコンテンツ配信処理例１におけるコンテンツ配信サーバの処理を説明するフローチャートを示す図である。

図６は、本発明のコンテンツ配信システムのコンテンツ配信処理例１におけるダウンロード先の装置であるホームＰＣの処理を説明するフローチャートを示す図である。

図７は、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例２の処理シーケンスを説明する図である。

図８は、本発明のコンテンツ配信システムのコンテンツ配信処理例２におけるダウンロード要求装置である携帯情報端末の処理を説明するフローチャートを示す図である。

図９は、本発明のコンテンツ配信システムのコンテンツ配信処理例２におけるコンテンツ配信サーバの処理を説明するフローチャートを示す図である。

図１０は、本発明のコンテンツ配信システムのコンテンツ配信処理例２におけるダウンロード先の装置であるホームＰＣの処理を説明するフローチャートを示

す図である。

図１１は、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例３の処理シーケンスを説明する図である。

図１２は、本発明のコンテンツ配信システムのコンテンツ配信処理例３におけるダウンロード要求装置である携帯情報端末の処理を説明するフローチャートを示す図である。

図１３は、本発明のコンテンツ配信システムのコンテンツ配信処理例３におけるコンテンツ配信サーバの処理を説明するフローチャートを示す図である。

図１４は、本発明のコンテンツ配信システムのコンテンツ配信処理例３におけるダウンロード先の装置であるホームＰＣの処理を説明するフローチャートを示す図である。

図１５は、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例４の処理シーケンスを説明する図である。

図１６は、本発明のコンテンツ配信システムのコンテンツ配信処理例４におけるダウンロード要求装置である携帯情報端末の処理を説明するフローチャートを示す図である。

図１７は、本発明のコンテンツ配信システムのコンテンツ配信処理例４におけるコンテンツ配信サーバの処理を説明するフローチャートを示す図である。

図１８は、本発明のコンテンツ配信システムのコンテンツ配信処理例４におけるダウンロード先の装置であるホームＰＣの処理を説明するフローチャートを示す図である。

図１９は、本発明のコンテンツ配信システムにおけるホームＰＣ、携帯情報端末等の情報処理装置の構成例を示す図である。

図２０は、本発明のコンテンツ配信システムにおけるコンテンツ配信サーバの構成例を示す図である。

発明を実施するための最良の形態

［システム概要］

図１に本発明のコンテンツ配信システムが適用可能なコンテンツ配信構成例を

示す。コンテンツの配信は、コンテンツ配信サーバ１５０が様々なユーザ機器に対して実行する。図１には、ユーザサイト１１０にユーザの所有する複数の情報端末を示している。ホームＰＣ１２０は、例えばハードディスク等の大容量の記憶媒体（ホームストレージ（ＨＳ））を有し、ユーザの自宅に備えられた情報処理装置である。また、ユーザサイト１１０には、携帯電話、ＰＤＡ等の携帯情報端末１３０があり、これらの携帯情報端末１３０は、例えばユーザの外出時等に携帯可能なモバイル型の情報処理装置である。

ユーザは、ホームストレージを有するホームＰＣ１２０、携帯情報端末１３０のそれぞれを用いて、コンテンツ配信サーバ１５０にアクセスし、各接続機器とコンテンツ配信サーバ１５０間において認証処理、例えば公開鍵暗号方式、または共通鍵暗号方式等に従った認証を実行し、機器の正当性、すなわち、コンテンツ配信サーバがコンテンツの利用を認めた機器であるかを確認して、確認の後、コンテンツの送信、ダウンロード処理を実行する。これらの処理は、ダウンロード対象となる機器との直接認証であり、従来と同様の処理である。

さらに、本発明のシステムでは、例えば携帯情報端末１３０からコンテンツ配信サーバ１５０にアクセスを実行し、コンテンツ送信、ダウンロード処理先として、携帯情報端末１３０ではなく、ホームＰＣ１２０を指定して、コンテンツ配信サーバ１５０からホームＰＣ１２０に対するコンテンツ送信、ホームＰＣ１２０におけるダウンロードを実行可能とする。

例えば、外出先で携帯電話を利用するユーザが、携帯電話を利用してコンテンツ配信サーバにアクセスして、映画等の動画像データのような大容量コンテンツのダウンロード先としてホームＰＣを指定して、コンテンツ配信サーバからホームＰＣに対する動画像コンテンツの送信、ダウンロード処理を実行させる。

従来、コンテンツ配信サーバ１５０は、ダウンロード対象機器に対する認証の成立を条件としてコンテンツを送信ダウンロード処理の実行を可能としていた。本発明のシステムでは、携帯情報端末１３０を利用するユーザが携帯情報端末１３０を利用してコンテンツ配信サーバ１５０にアクセスし、ホームＰＣ１２０に変わってホームＰＣが信用できるユーザ機器であり、正当なコンテンツ利用権を持つ機器であることの証明処理としての代理認証を実行する。コンテンツ配信サ

ーバ１５０は、この代理認証の成立を条件として、ホームＰＣ１２０に対するコンテンツ送信を実行する。

図１に示す、ホームＰＣ１２０と、携帯情報端末１３０のように、コンテンツ配信サーバに対するアクセス機器、および該アクセス機器からコンテンツのダウンロード先として指定可能な機器、これらの複数のユーザ機器は、予め、相互にデバイス証明書となるデバイスチケットを交換し、またこれらのユーザ機器における共有秘密鍵としてのホームネットエリア共有秘密鍵を各機器の記憶手段に格納する。

図２にユーザ機器の格納情報、およびユーザ機器間で実行される処理を説明する図を示す。なお、以下の説明におけるデータ、あるいは式等の表示として、携帯情報端末をＭＢＬ（Ｍｏｂｉｌｅ）、ホームＰＣをＨＳ（Ｈｏｍｅ　Ｓｔｏｒａｇｅ）として略記する。

携帯情報端末１３０は、製造時に各機器にユニークな識別子としての機器ＩＤ［ＩＤ＿ＭＢＬ］が割り当てられ、各機器のメモリに格納される。この機器ＩＤは書き換え不可能な固定ＩＤである。また、通信のためのアドレス、例えばＩＰｖ６に従ったＩＰアドレス［ＡＤＤ＿ＭＢＬ］が設定される。

インターネットにおいて、通信プロトコルとしてＩＰ(Internet Protocol)が用いられ、現在多く使用されているＩＰはＩＰｖ４であり、これは発信元／宛先として３２ビットからなるアドレス（ＩＰアドレス）である。しかし、ＩＰｖ４の限られたアドレス空間、すなわちグローバルアドレスの枯渇が問題となっており、これを解決するのが、ＩＰアドレス空間を３２ビットから１２８ビットに拡張したＩＰｖ６(Internet Protocol version 6)である。ＩＰｖ６アドレスは、上位６４ビットの経路情報（ネットワークプレフィックス：Network Prefix）［ＡＤＤ＿ＮＥＴ＿Ａ］と、下位６４ビットの、個々の通信端末、すなわちホストを識別するホストアドレスとから構成される。上述の機器ＩＤ［ＩＤ＿ＭＢＬ］をＩＰｖ６アドレスの下位ビットのホストアドレスとして利用し、ＩＰアドレス[ＡＤＤ＿ＭＢＬ]を［ＡＤＤ＿ＮＥＴ＿Ａ｜ＩＤ＿ＭＢＬ］として設定することができる。

さらに、携帯情報端末１３０は、コンテンツ配信に係る決済処理の際の認証を

行なう決済サービス用認証サーバ（ＣＲ）から発行されるユーザ証明書［Ｃｅｒｔ＿Ｕｓｅｒ］を有する。ユーザ証明書は、コンテンツ配信サーバからのコンテンツダウンロードサービスを行なおうとするユーザが、決済処理に必要な情報を決済サービス用認証サーバ（ＣＲ）に届け出ることにより、決済サービス用認証サーバ（ＣＲ）が発行する証明書である。

ユーザ証明書［Ｃｅｒｔ＿Ｕｓｅｒ］は、ユーザＩＤ［ＩＤ＿ＵＳＲ］と、ユーザの公開鍵［Ｋ＿ＰＵＢ＿ＵＳＲ］とをメッセージとして、決済サービス用認証サーバ（ＣＲ）の秘密鍵［Ｋ＿ＳＥＣ＿ＣＲ］で電子署名をしたデータ、すなわち、［Ｃｅｒｔ＿Ｕｓｅｒ］＝［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＣＲ，（ＩＤ＿ＵＳＲ，Ｋ＿ＰＵＢ＿ＵＳＲ））］である。なお、電子署名は、例えば、一方向性関数としてのハッシュ関数を適用し、所定の鍵に基づいてハッシュ関数を実行することによって生成されるハッシュ値が用いられる。なお、Ｓｉｇ（Ａ，Ｂ）は、Ａを適用したＢに対する電子署名データを意味するものとする。

電子署名の付与されたデータを受信した受信者は、自己の所有する鍵に基づいて同様にハッシュ値を算出し、データに付与されているハッシュ値との一致を判定することでデータの改竄のないことを確認することができる。

携帯情報端末１３０は、決済サービス用認証サーバ（ＣＲ）から発行されるユーザ証明書［Ｃｅｒｔ＿Ｕｓｅｒ］を自己の所有する秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］で署名して、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｃｅｒｔ＿Ｕｓｅｒ）］としてメモリに保存する。

一方、ホームＰＣ１２０は、製造時に各機器にユニークな識別子としての機器ＩＤ［ＩＤ＿ＨＳ］が割り当てられ、メモリに格納される。この機器ＩＤは書き換え不可能な固定ＩＤである。また、通信のためのアドレス、例えばＩＰｖ６に従ったＩＰアドレス［ＡＤＤ＿ＨＳ］が設定される。このアドレスは、上述の携帯情報端末のアドレスと同様、ＩＰｖ６アドレスの上位６４ビットの経路情報(ネットワークプレフィックス：Network Prefix）［ＡＤＤ＿ＮＥＴ＿Ｂ］に、下位６４ビットとしての上述の機器ＩＤ［ＩＤ＿ＨＳ］を利用し、［ＡＤＤ＿ＨＳ］を［ＡＤＤ＿ＮＥＴ＿Ｂ｜ＩＤ＿ＨＳ］として設定することができる。

さらに、ホームＰＣ１２０は、携帯情報端末１３０と同様、コンテンツ配信に

係る決済処理の際の認証を行なう決済サービス用認証サーバ（ＣＲ）から発行されるユーザ証明書［Ｃｅｒｔ＿Ｕｓｅｒ］を格納する。ホームＰＣ１２０は、この決済サービス用認証サーバ（ＣＲ）から発行されるユーザ証明書［Ｃｅｒｔ＿Ｕｓｅｒ］を自己の所有する秘密鍵［Ｋ＿ＳＥＣ＿ＨＳ］で署名して、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，Ｃｅｒｔ＿Ｕｓｅｒ）］としてメモリに保存する。

さらに、ホームＰＣ１２０は、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有する。このホームネットエリア共有秘密鍵［Ｋｓｅｃ］は、上述したコンテンツ配信サーバとの代理認証を実行するアクセス機器（ここでは携帯情報端末１３０）に対して必要に応じて送信され、アクセス機器にも格納される。

携帯情報端末１３０、ホームＰＣ１２０は、それぞれ上述したデータをそれぞれの記憶手段としてのメモリに格納しているが、上述したコンテンツ配信サーバからの他機器に対するダウンロードサービスを実行するために、図２に示すデータ２０１をホームＰＣ１２０から携帯情報端末１３０に送信し、データ２０２を携帯情報端末１３０からホームＰＣ１２０に対して送信する。

このデータの送受信は、２者間で同じホームネットエリアに属することを個人認証等の手段を通して確認した上で行われ、他の個所にチケットが流出してはならない。交換されたチケットは、公開鍵ペアの秘密鍵を用いて受け取り手の署名を付加することにより、安全に保持される。

ホームＰＣ１２０から携帯情報端末１３０に送信されるデータ２０１は、ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］、およびホームネットエリア共有秘密鍵［Ｋｓｅｃ］である。また、携帯情報端末１３０からホームＰＣ１２０に対して送信されるデータ２０２は、携帯情報端末チケット［Ｔｉｃｋｅｔ＿ＭＢＬ］である。

機器Ａから機器Ｂに対して発行されるチケットは、機器ＡのＩＤ［ＩＤ＿Ａ］と、機器ＢのＩＤ［ＩＤ＿Ｂ］と、機器Ａの公開鍵［Ｋ＿ＰＵＢ＿Ａ］をメッセージとして、該メッセージに機器Ａの秘密鍵［Ｋ＿ＳＥＣ＿Ａ］で電子署名をしたデータ、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿Ａ，（ＩＤ＿Ａ，ＩＤ＿Ｂ，Ｋ＿ＰＵＢ＿Ａ））］である。

すなわち、ホームＰＣ１２０から携帯情報端末１３０に送信されるデータ２０

１としてのホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］は、ホームＰＣ１２０のＩＤ［ＩＤ＿ＨＳ］と、携帯情報端末１３０のＩＤ［ＩＤ＿ＭＢＬ］と、ホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］をメッセージとして、該メッセージにホームＰＣ１２０の秘密鍵［Ｋ＿ＳＥＣ＿ＨＳ］で電子署名をしたデータ、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，（ＩＤ＿ＨＳ，ＩＤ＿ＭＢＬ，Ｋ＿ＰＵＢ＿ＨＳ））］である。ホームＰＣ１２０から携帯情報端末１３０には、このホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］と、さらにホームネットエリア共有秘密鍵［Ｋｓｅｃ］が送信される。

なお、後段で説明するコンテンツ配信処理例３，４では、公開鍵、秘密鍵ペアをＫｓｅｃの代わりに利用する方式であり、通常の公開鍵の利用法式と異なる方式を採用している。すなわち、例えばＫｓｅｃの代わりに利用される公開鍵ペアは専用に別に用意され、ホームエリア内にのみ公開鍵が公開される。これにより、Ｋｓｉｇを取得できるのは、ホームエリア内の機器のみとなる。本方式は、Ｋｓｅｃを共有する構成と異なり、機器毎に個別の秘密鍵を持つので、個別の機器をセキュリティ的に区別した利用形態に適している。

一方、携帯情報端末１３０からホームＰＣ１２０に送信されるデータ２０２としての携帯情報端末チケット［Ｔｉｃｋｅｔ＿ＭＢＬ］は、携帯情報端末１３０のＩＤ［ＩＤ＿ＭＢＬ］と、ホームＰＣ１２０のＩＤ［ＩＤ＿ＨＳ］と、携帯情報端末１３０の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］をメッセージとして、該メッセージに携帯情報端末１３０の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］で電子署名をしたデータ、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，（ＩＤ＿ＭＢＬ，ＩＤ＿ＨＳ，Ｋ＿ＰＵＢ＿ＭＢＬ））］である。

携帯情報端末１３０は、ホームＰＣ１２０から送信されるホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］と、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］をメモリに格納し、一方、ホームＰＣ１２０は、携帯情報端末１３０から送信される携帯情報端末チケット［Ｔｉｃｋｅｔ＿ＭＢＬ］をメモリに格納する。

図２の構成において、携帯情報端末１３０は、自装置と異なるダウンロード先としてホームＰＣ１２０を指定したコンテンツダウンロード要求を実行する情報処理装置であり、コンテンツのダウンロード先としての情報処理装置（ホームＰ

Ｃ１２０）の電子署名がなされたチケットを記憶手段としてのメモリに格納し、携帯情報端末１３０のＣＰＵ等の制御手段において、メモリに格納したチケットを含むコンテンツダウンロード要求コマンドを生成し、生成したコンテンツダウンロード要求コマンドを通信手段を介してコンテンツ配信サーバに対して送信する。以下、本発明のシステムにおけるコンテンツ配信処理の詳細について説明する。

［コンテンツ配信処理例１］

以下、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例について、複数の処理態様を順次、説明する。なお、以下の説明では、携帯情報端末がコンテンツ配信サーバにアクセスを実行して、ホームストレージを備えたホームＰＣに対するコンテンツダウンロードを実行する処理として説明するが、この逆の処理、すなわち、ホームＰＣからコンテンツ配信サーバにアクセスを実行し、携帯情報端末に対してコンテンツのダウンロードを実行することも同様の処理過程を実行することで可能であり、ユーザ所有の端末のコンテンツ配信サーバに対するアクセス処理端末､ダウンロード処理端末は任意の組み合わせが可能である。

まず、図３乃至図６を参照して、コンテンツ配信処理例１について説明する。図３は、コンテンツ配信サーバとコンテンツ配信サーバに対するアクセスを実行する携帯情報端末と、携帯情報端末からの要求に従って、コンテンツをダウンロードする大容量記憶媒体としてのホームストレージを備えたホームＰＣとの３者間で実行する処理を示すシーケンス図である。図４は携帯情報端末の処理を示すフローチャート、図５はコンテンツ配信サーバの処理を示すフローチャート、図６はホームＰＣの処理を示すフローチャートである。

図３を参照して、本実施例の処理について説明する。図３において処理は、図に示す番号（１）～（９）の順に進行する。

また、図３において、携帯情報端末１３０の識別子（ＩＤ）は［ＩＤ＿ＭＢＬ］、アドレスは［ＡＤＤ＿ＭＢＬ］であり、これは、［ＡＤＤ＿ＮＥＴ＿Ａ｜ＩＤ＿ＭＢＬ］に相当する。また、携帯情報端末１３０は、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有する。また、ホームＰＣ１２０の識別子（ＩＤ）は［ＩＤ

＿ＨＳ］、アドレスは［ＡＤＤ＿ＨＳ］であり、これは、［ＡＤＤ＿ＮＥＴ＿Ｂ｜ＩＤ＿ＨＳ］に相当する。また、ホームＰＣ１２０は、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有する。また、コンテンツ配信サーバ１５０の識別子（ＩＤ）は［ＩＤ＿ＳＲＶ］、アドレスは［ＡＤＤ＿ＳＲＶ］であり、これは、［ＡＤＤ＿ＮＥＴ＿Ｘ｜ＩＤ＿ＳＲＶ］に相当するものとする。

まず、（１）の処理として、携帯情報端末１３０は、コンテンツ配信サーバ１５０に対して、コンテンツのダウンロードを要求する。このダウンロード要求には、ダウンロード先となる機器、ここではホームＰＣ１２０から受領したホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］、および、ダウンロード先となるホームＰＣ１２０の公開鍵を格納した公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］が含まれる。なお、公開鍵証明書は、別途認証局（ＣＡ）から取得する構成としてもよい。ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］は、ホームＰＣ１２０のＩＤ［ＩＤ＿ＨＳ］と、携帯情報端末１３０のＩＤ［ＩＤ＿ＭＢＬ］と、ホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］をメッセージとして、該メッセージにホームＰＣ１２０の秘密鍵［Ｋ＿ＳＥＣ＿ＨＳ］で電子署名をしたデータ、すなわち、［Ｓｉｇ(Ｋ＿ＳＥＣ＿ＨＳ,(ＩＤ＿ＨＳ,ＩＤ＿ＭＢＬ,Ｋ＿ＰＵＢ＿ＨＳ))］である。

携帯情報端末１３０からホームＰＣチケット［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，（Ｔｉｃｋｅｔ＿ＨＳ））］、ホームＰＣ１２０の公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］を受信したコンテンツ配信サーバ１５０は、携帯情報端末１３０の公開鍵証明書から取得される携帯情報端末１３０の公開鍵を用いて、ホームＰＣチケット［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，（Ｔｉｃｋｅｔ＿ＨＳ））］の署名検証を実行し、（２）の処理としてホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証処理を実行する。この検証処理の手順は、（ａ）ホームＰＣ１２０の公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］の署名（認証局署名）検証による公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］の正当性確認処理、（ｂ）正当性の確認された公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］からのホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］の取得処理、（ｃ）取得したホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］を適用したホームＰＣチケット［Ｔｉｃｋｅｔ＿Ｈ

Ｓ］、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，（ＩＤ＿ＨＳ，ＩＤ＿ＭＢＬ，Ｋ＿ＰＵＢ＿ＨＳ））］の署名検証処理である。

この手続き、すなわちホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証により、ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］が改竄の無い正当なチケットであることが確認されると、コンテンツ配信サーバ１５０は、（３）の処理として、コンテンツ署名用鍵［Ｋｓｉｇ］を生成する。これは例えば乱数発生器により生成される乱数に基づいて生成する一時的に使用するための鍵である。次に、（４）の処理として、コンテンツ配信サーバ１５０は、生成したコンテンツ署名用鍵［Ｋｓｉｇ］を携帯情報端末１３０に送信する。

コンテンツ署名用鍵［Ｋｓｉｇ］を受信した携帯情報端末１３０は、（５）の処理として、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用してコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化して、暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を生成する。この暗号化処理には、例えばＤＥＳ暗号化処理が適用される。なお、Ｅ（Ａ，Ｂ）は、ＢをＡによって暗号化したデータを示すものとする。次に、携帯情報端末１３０は、（６）の処理として、生成した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］をコンテンツ配信サーバ１５０に送信する。

（７）の処理として、コンテンツ配信サーバ１５０は、先に生成したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、ダウンロード対象のコンテンツ（Ｍ）に対する電子署名を行ない、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ）］を生成する。

次に（８）の処理として、コンテンツ配信サーバ１５０は、ダウンロード先となるホームＰＣ１２０に対して、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ）］と、先の（５）の処理において、携帯情報端末１３０から受信した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を送信する。

次に、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ）］と、暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を受信したホームＰＣ１２０は、（９）の処理として、自己の所有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、受信した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］の復号処理を実行して、コンテンツ署名用鍵［Ｋｓｉｇ］を取り出して、署名されたコンテ

ンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ）］の署名検証処理を実行する。この署名検証処理において、コンテンツ（Ｍ）のデータ改竄のないことが立証されたことを条件としてコンテンツの格納または再生処理を実行する。

次に、図４乃至図６のフローチャートを参照して、携帯情報端末１３０の処理、コンテンツ配信サーバ１５０の処理、およびホームＰＣ１２０の処理のそれぞれについて説明する。

まず、図４のフローチャートを参照して携帯情報端末１３０の処理手順について説明する。ステップＳ１１１において、携帯情報端末１３０は、ダウンロード先となる機器のデバイスチケット、ここではホームＰＣ１２０のホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むデータをコンテンツ配信サーバ１５０に送信して、コンテンツのダウンロードを要求する。

ステップＳ１１２において、携帯情報端末１３０は、コンテンツ配信サーバ１５０の生成したコンテンツ署名用鍵［Ｋｓｉｇ］を受信する。

ステップＳ１１３において、コンテンツ署名用鍵［Ｋｓｉｇ］を受信した携帯情報端末１３０は、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用してコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化して、暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を生成し、ステップＳ１１４において、生成した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］をコンテンツ配信サーバ１５０に送信する。

以上の処理が、携帯情報端末１３０とコンテンツ配信サーバ１５０間で実行されるコンテンツダウンロード要求処理における携帯情報端末１３０側の処理である。

次に、図５を参照して、携帯情報端末１３０からコンテンツダウンロード要求コマンドを受信するコンテンツ配信サーバ１５０の処理について説明する。

まず、コンテンツ配信サーバ１５０は、ステップＳ１２１において、携帯情報端末１３０から、ダウンロード先のデバイスチケット、ここではホームＰＣ１２０のホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むデータをダウンロードコマンドとして受信する。

携帯情報端末１３０からホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むダウンロードコマンドを受信したコンテンツ配信サーバ１５０は、ステップＳ１２

２において、ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証処理を実行する。この検証処理は、先に説明したように、ホームＰＣ１２０の公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］の署名（認証局署名）検証による公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］の正当性確認処理、正当性の確認された公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］からのホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］の取得処理、得したホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］を適用したホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，（ＩＤ＿ＨＳ，ＩＤ＿ＭＢＬ，Ｋ＿ＰＵＢ＿ＨＳ））］の署名検証処理を順次行なうことによって実行される。

ステップＳ１２３において、チケット検証が不成立と判定された場合は、チケット、すなわちホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］が偽造されたものである可能性があり、ステップＳ１２９に進み、エラーメッセージを携帯情報端末１３０に送信して処理を終了する。この場合は、コンテンツのダウンロード処理は実行されない、

ステップＳ１２３において、チケット検証が成立したと判定された場合は、ステップＳ１２４に進み、コンテンツ署名用鍵［Ｋｓｉｇ］を生成し、ステップＳ１２５において、生成したコンテンツ署名用鍵［Ｋｓｉｇ］を携帯情報端末１３０に送信する。

次に、コンテンツ配信サーバ１５０は、ステップＳ１２６において、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用してコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を携帯情報端末１３０から受信する。

次に、コンテンツ配信サーバ１５０は、ステップＳ１２７において、先に生成したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、ダウンロード対象のコンテンツ（Ｍ）に対する電子署名を行ない、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ）］を生成する。

次に、コンテンツ配信サーバ１５０は、ステップＳ１２８において、ダウンロード先となるホームＰＣ１２０に対して、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ)］と、先に携帯情報端末１３０から受信した暗号化鍵デ

ータ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ)］を送信する。

以上の処理が、携帯情報端末１３０からコンテンツダウンロード要求を受信した配信サーバ１５０の処理である。

次に、図６を参照して、コンテンツ配信サーバ１５０からコンテンツのダウンロードが実行されるホームＰＣ１２０の処理について説明する。

ホームＰＣ１２０は、ステップＳ１３１において、コンテンツ配信サーバ１５０から、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ)］と、暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ)］を受信する。

ステップＳ１３２において、ホームＰＣ１２０は、自己の所有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、受信した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ)］の復号処理を実行する。

ステップＳ１３３において、復号に失敗した場合は、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］が携帯情報端末１３０の有する鍵と異なるなど、正当なホームネットエリア共有秘密鍵でない可能性があり、ステップＳ１３７に進み、受信コンテンツを破棄する。

ステップＳ１３３において、復号に成功した場合は、復号によって取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ)］の署名検証処理を実行する。この署名検証に不成功の場合（Ｓ１３５でＮｏ）は、コンテンツ改竄の可能性があり、ステップＳ１３７に進み、受信コンテンツを破棄する。

署名検証に成功した場合（Ｓ１３５でＹｅｓ）は、ステップＳ１３６において、受信コンテンツをホームＰＣ１２０のストレージに格納し、ダウンロード処理を終了する。

以上の処理が、携帯情報端末１３０からコンテンツダウンロード要求を受信した配信サーバ１５０からのコンテンツを受信し、ダウンロードを実行するホームＰＣ１２０の処理である。

上述したように、本実施例においては、コンテンツ配信サーバ１５０は、携帯情報端末１３０から受信したコンテンツダウンロード先のデバイスチケットの検証が可能となり、携帯情報端末１３０の送付してきたホームＰＣチケットに基づ

いて、ホームＰＣ１２０が、携帯情報端末１３０の承認しているダウンロード先であることの確認が可能となる。

すなわち、本発明の構成によれば、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツダウンロード先のデバイスによる署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホームＰＣが、携帯情報端末の承認しているダウンロード先である確認が可能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。

また、本実施例においては、コンテンツ署名用鍵［Ｋｓｉｇ］を、ホームＰＣ１２０と携帯情報端末１３０の共有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］により暗号化して、携帯情報端末１３０からコンテンツ配信サーバ１５０を介してダウンロード先であるホームＰＣ１２０に送信し、ホームＰＣ１２０において所有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］により復号してコンテンツ署名用鍵［Ｋｓｉｇ］を取得する構成としたので、ホームＰＣ１２０と携帯情報端末１３０が同一のホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有することが、ダウンロード先であるホームＰＣ１２０においてコンテンツ署名用鍵［Ｋｓｉｇ］を取得できる条件となり、同一のホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有する機器間においてのみ、有効なコンテンツのダウンロードが実行可能となる。

［コンテンツ配信処理例２］

次に、コンテンツ配信処理例２について説明する。コンテンツ配信処理例２は、コンテンツ配信サーバ１５０がコンテンツのハッシュ値を算出して、ハッシュ値をホームＰＣ１２０と携帯情報端末１３０が有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］で暗号化して、携帯情報端末１３０からコンテンツ配信サーバ１５０を介してダウンロード先であるホームＰＣ１２０に送信する処理を実行する構成例である。

図７乃至図１０を参照して、コンテンツ配信処理例２について説明する。図７

は、コンテンツ配信サーバとコンテンツ配信サーバに対するアクセスを実行する携帯情報端末と、携帯情報端末からの要求に従って、コンテンツをダウンロードする大容量記憶媒体としてのホームストレージを備えたホームＰＣとの３者間で実行する処理を示すシーケンス図である。図８は携帯情報端末の処理を示すフローチャート、図９はコンテンツ配信サーバの処理を示すフローチャート、図１０はホームＰＣの処理を示すフローチャートである。

図７を参照して、本実施例の処理について説明する。図７において処理は、図に示す番号（１）～（９）の順に進行する。

まず、（１）の処理として、携帯情報端末１３０は、コンテンツ配信サーバ１５０に対して、コンテンツのダウンロードを要求する。このダウンロード要求には、ダウンロード先となる機器、ここではホームＰＣ１２０から受領したホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］、および、ダウンロード先となるホームＰＣ１２０の公開鍵を格納した公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］が含まれる。ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］は、ホームＰＣ１２０のＩＤ［ＩＤ＿ＨＳ］と、携帯情報端末１３０のＩＤ［ＩＤ＿ＭＢＬ］と、ホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］をメッセージとして、該メッセージにホームＰＣ１２０の秘密鍵［Ｋ＿ＳＥＣ＿ＨＳ］で電子署名をしたデータ、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，（ＩＤ＿ＨＳ，ＩＤ＿ＭＢＬ，Ｋ＿ＰＵＢ＿ＨＳ））］である。

携帯情報端末１３０からホームＰＣチケット［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，（Ｔｉｃｋｅｔ＿ＨＳ））］、ホームＰＣ１２０の公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］を受信したコンテンツ配信サーバ１５０は、携帯情報端末１３０の公開鍵証明書から取得される携帯情報端末１３０の公開鍵を用いて、ホームＰＣチケット［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，（Ｔｉｃｋｅｔ＿ＨＳ））］の署名検証を実行し、（２）の処理としてホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証処理を実行する。この検証処理の手順は、（ａ）ホームＰＣ１２０の公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］の署名（認証局署名）検証による公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］の正当性確認処理、（ｂ）正当性の確認された公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］からのホームＰＣ１２０の公開鍵［Ｋ＿

ＰＵＢ＿ＨＳ］の取得処理、（ｃ）取得したホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］を適用したホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，（ＩＤ＿ＨＳ，ＩＤ＿ＭＢＬ，Ｋ＿ＰＵＢ＿ＨＳ））］の署名検証処理である。

この手続き、すなわちホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証により、ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］が改竄の無い正当なチケットであることが確認されると、コンテンツ配信サーバ１５０は、（３）の処理として、コンテンツのハッシュ値［Ｈ（Ｍ）］を計算する。次に、（４）の処理として、コンテンツ配信サーバ１５０は、生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を携帯情報端末１３０に送信する。

コンテンツのハッシュ値［Ｈ（Ｍ）］を受信した携帯情報端末１３０は、（５）の処理として、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用してコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化して、暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を生成し、（６）の処理として、生成した暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］をコンテンツ配信サーバ１５０に送信する。

（７）の処理として、コンテンツ配信サーバ１５０は、暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］とコンテンツ（Ｍ）からなるコンテンツパッケージ［Ｍ｜Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を生成し、（８）の処理として、コンテンツ配信サーバ１５０は、ダウンロード先となるホームＰＣ１２０に対して、コンテンツパッケージ［Ｍ｜Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を送信する。

次に、コンテンツパッケージ［Ｍ｜Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を受信したホームＰＣ１２０は、（９）の処理として、自己の所有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、受信したコンテンツパッケージ［Ｍ｜Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］に含まれる暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］の復号処理を実行して、コンテンツ署名用鍵［Ｋｓｉｇ］を取り出して、コンテンツのハッシュ値［Ｈ（Ｍ）］を取り出し、また、コンテンツ（Ｍ）に対するハッシュ値を計算して、両ハッシュ値の一致を確認する。一致している場合は、コンテンツの改竄がないと判定し、不一致の場合は、コンテンツ改竄ありと判定する。検証処理において、コンテンツ（Ｍ）のデータ改竄のないことが立証されたことを条

件としてコンテンツの格納または再生処理を実行する。

次に、図８乃至図１０のフローチャートを参照して、携帯情報端末１３０の処理、コンテンツ配信サーバ１５０の処理、およびホームＰＣ１２０の処理のそれぞれについて説明する。

まず、図８のフローチャートを参照して携帯情報端末１３０の処理手順について説明する。ステップＳ２１１において、携帯情報端末１３０は、ダウンロード先となる機器のデバイスチケット、ここではホームＰＣ１２０のホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むデータをコンテンツ配信サーバ１５０に送信して、コンテンツのダウンロードを要求する。

ステップＳ２１２において、携帯情報端末１３０は、コンテンツ配信サーバ１５０の生成したコンテンツのハッシュ値［Ｈ（Ｍ)］を受信する。

ステップＳ２１３において、コンテンツのハッシュ値［Ｈ（Ｍ)］を受信した携帯情報端末１３０は、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用してコンテンツのハッシュ値［Ｈ（Ｍ)］を暗号化して、暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ))］を生成し、ステップＳ２１４において、生成した暗号化ハッユ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ))］をコンテンツ配信サーバ１５０に送信する。

以上の処理が、携帯情報端末１３０とコンテンツ配信サーバ１５０間で実行されるコンテンツダウンロード要求処理における携帯情報端末１３０側の処理である。

次に、図９を参照して、携帯情報端末１３０からコンテンツダウンロード要求コマンドを受信するコンテンツ配信サーバ１５０の処理について説明する。

まず、コンテンツ配信サーバ１５０は、ステップＳ２２１において、携帯情報端末１３０から、ダウンロード先のデバイスチケット、ここではホームＰＣ１２０のホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むデータをダウンロードコマンドとして受信する。

携帯情報端末１３０からホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むダウンロードコマンドを受信したコンテンツ配信サーバ１５０は、ステップＳ２２２において、ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証処理を実行する。この検証処理は、先に説明したと同様の処理である。

ステップＳ２２３において、チケット検証が不成立と判定された場合は、チケット、すなわちホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］が偽造されたものである可能性があり、ステップＳ２２９に進み、エラーメッセージを携帯情報端末１３０に送信して処理を終了する。この場合は、コンテンツのダウンロード処理は実行されない、

ステップＳ２２３において、チケット検証が成立したと判定された場合は、ステップＳ２２４に進み、コンテンツのハッシュ値［Ｈ（Ｍ）］を生成し、ステップＳ２２５において、生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を携帯情報端末１３０に送信する。

次に、コンテンツ配信サーバ１５０は、ステップＳ２２６において、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用してコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を携帯情報端末１３０から受信する。

次に、コンテンツ配信サーバ１５０は、ステップＳ２２７において、携帯情報端末１３０から受信した暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］とコンテンツ（Ｍ）からなるコンテンツパッケージ［Ｍ｜Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を生成する。

次に、コンテンツ配信サーバ１５０は、スイテップＳ２２８において、ダウンロード先となるホームＰＣ１２０に対して、コンテンツパッケージ［Ｍ｜Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を送信する。

以上の処理が、携帯情報端末１３０からコンテンツダウンロード要求を受信した配信サーバ１５０の処理である。

次に、図１０を参照して、コンテンツ配信サーバ１５０からコンテンツのダウンロードが実行されるホームＰＣ１２０の処理について説明する。

ホームＰＣ１２０は、ステップＳ２３１において、コンテンツ配信サーバ１５０から、コンテンツパッケージ［Ｍ｜Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を受信する。

ステップＳ２３２において、ホームＰＣ１２０は、自己の所有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、受信したコンテンツパッケージ［Ｍ｜Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］に含まれる暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］

の復号処理を実行する。

ステップＳ２３３において、復号に失敗した場合は、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］が携帯情報端末１３０の有する鍵と異なるなど、正当なホームネットエリア共有秘密鍵でない可能性があり、ステップＳ２３７に進み、受信コンテンツを破棄する。

ステップＳ２３３において、復号に成功した場合は、復号によって取得したコンテンツのハッシュ値［Ｈ（Ｍ)］と、コンテンツ（Ｍ）に基づいて計算により算出したハッシュ値Ｈ（Ｍ)’との比較を実行する。この比較において両ハッシュ値が不一致の場合（Ｓ２３５でＮｏ）は、コンテンツ改竄の可能性があり、ステップＳ２３７に進み、受信コンテンツを破棄する。

両ハッシュ値が一致した場合（Ｓ２３５でＹｅｓ）は、ステップＳ２３６において、受信コンテンツをホームＰＣ１２０のストレージに格納し、ダウンロード処理を終了する。

以上の処理が、携帯情報端末１３０からコンテンツダウンロード要求を受信した配信サーバ１５０からのコンテンツを受信し、ダウンロードを実行するホームＰＣ１２０の処理である。

上述したように、本実施例においては、コンテンツ配信サーバ１５０は、携帯情報端末１３０から受信したコンテンツダウンロード先のデバイスチケットの検証が可能となり、携帯情報端末１３０の送付してきたホームＰＣチケットに基づいて、ホームＰＣ１２０が、携帯情報端末１３０の承認しているダウンロード先であることの確認が可能となる。すなわち、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツダウンロード先のデバイスによる署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホームＰＣが、携帯情報端末の承認しているダウンロード先である確認が可能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。

また、本実施例においては、コンテンツのハッシュ値［Ｈ（Ｍ)］を、ホームＰＣ１２０と携帯情報端末１３０の共有するホームネットエリア共有秘密鍵［Ｋｓ

ｅｃ］により暗号化して、携帯情報端末１３０からコンテンツ配信サーバ１５０を介してダウンロード先であるホームＰＣ１２０に送信し、ホームＰＣ１２０において所有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］により復号してコンテンツのハッシュ値［Ｈ（Ｍ)］を取得して、コンテンツに基づいてみずから算出するハッシュ値と比較する構成としたので、ホームＰＣ１２０と携帯情報端末１３０が同一のホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有することが、ダウンロード先であるホームＰＣ１２０においてハッシュ値の比較できる条件となり、同一のホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有する機器間においてのみ、有効なコンテンツのダウンロードが実行可能となる。

［コンテンツ配信処理例３］

次に、コンテンツ配信処理例３について説明する。コンテンツ配信処理例３は、コンテンツ配信処理例１，２で適用したホームネットエリア共有秘密鍵［Ｋｓｅｃ］を用いず、一般的な公開鍵方式における公開鍵と秘密鍵の一の鍵を適用した処理を実行する構成例である。コンテンツ配信サーバ１５０がコンテンツの署名鍵を生成して、署名鍵の暗号化、復号化処理を公開鍵方式によりホームＰＣ１２０と携帯情報端末１３０において実行する例である。

図１１乃至図１４を参照して、コンテンツ配信処理例３について説明する。図１１は、コンテンツ配信サーバとコンテンツ配信サーバに対するアクセスを実行する携帯情報端末と、携帯情報端末からの要求に従って、コンテンツをダウンロードする大容量記憶媒体としてのホームストレージを備えたホームＰＣとの３者間で実行する処理を示すシーケンス図である。図１２は携帯情報端末の処理を示すフローチャート、図１３はコンテンツ配信サーバの処理を示すフローチャート、図１４はホームＰＣの処理を示すフローチャートである。

図１１を参照して、本実施例の処理について説明する。図１１において処理は、図に示す番号（１）～（９）の順に進行する。ホームＰＣ１２０と携帯情報端末１３０のそれぞれは、公開鍵方式の公開鍵、秘密鍵のペアを有する。すなわち、ホームＰＣ１２０は、［Ｋ＿ＰＵＢ＿ＨＳ］，［Ｋ＿ＳＥＣ＿ＨＳ］、携帯情報端末１３０は、［Ｋ＿ＰＵＢ＿ＭＢＬ］，［Ｋ＿ＳＥＣ＿ＭＢＬ］を有する。さらに、ダ

ウンロード先の機器であるホームＰＣ１２０は、ダウンロード要求処理を実行する機器、すなわち携帯情報端末１３０の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］を取得しているものとする。

まず、（１）の処理として、携帯情報端末１３０は、コンテンツ配信サーバ１５０に対して、コンテンツのダウンロードを要求する。このダウンロード要求には、ダウンロード先となる機器、ここではホームＰＣ１２０から受領したホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］、および、ダウンロード先となるホームＰＣ１２０の公開鍵を格納した公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］が含まれる。ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］は、ホームＰＣ１２０のＩＤ［ＩＤ＿ＨＳ］と、携帯情報端末１３０のＩＤ［ＩＤ＿ＭＢＬ］と、ホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］をメッセージとして、該メッセージにホームＰＣ１２０の秘密鍵［Ｋ＿ＳＥＣ＿ＨＳ］で電子署名をしたデータ、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，（ＩＤ＿ＨＳ，ＩＤ＿ＭＢＬ，Ｋ＿ＰＵＢ＿ＨＳ））］である。

携帯情報端末１３０からホームＰＣチケット［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，（Ｔｉｃｋｅｔ＿ＨＳ））］、ホームＰＣ１２０の公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］を受信したコンテンツ配信サーバ１５０は、携帯情報端末１３０の公開鍵証明書から取得される携帯情報端末１３０の公開鍵を用いて、ホームＰＣチケット［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，（Ｔｉｃｋｅｔ＿ＨＳ））］の署名検証を実行し、（２）の処理としてホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証処理を実行する。この検証処理の手順は、上述の処理例１と同様である。ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証により、ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］が改竄の無い正当なチケットであることが確認されると、コンテンツ配信サーバ１５０は、（３）の処理として、コンテンツ署名用鍵［Ｋｓｉｇ］を生成する。これは例えば乱数発生器により生成される乱数に基づいて生成する一時的に使用するための鍵である。次に、（４）の処理として、コンテンツ配信サーバ１５０は、生成したコンテンツ署名用鍵［Ｋｓｉｇ］を携帯情報端末１３０に送信する。

コンテンツ署名用鍵［Ｋｓｉｇ］を受信した携帯情報端末１３０は、（５）の処

理として、携帯情報端末１３０の第２秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］を適用してコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化して、暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ)］を生成する。携帯情報端末１３０の第２秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］は、チケットで使用される公開鍵ペアとは別の第２の公開鍵ペアを構成する秘密鍵である。この第２の公開鍵ペアは、ホームネットエリア内のみデ共有される秘密情報である。なお、携帯情報端末１３０の第２秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］を適用したコンテンツ署名用鍵［Ｋｓｉｇ］の暗号化処理は、公開鍵暗号方式による処理であり、秘密鍵で暗号化したデータはペアの公開鍵によって復号可能となる。次に、携帯情報端末１３０は、（６）の処理として、生成した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ)］をコンテンツ配信サーバ１５０に送信する。

（７）の処理として、コンテンツ配信サーバ１５０は、先に生成したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、ダウンロード対象のコンテンツ（Ｍ）に対する電子署名を行ない、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ)］を生成する。

次に（８）の処理として、コンテンツ配信サーバ１５０は、ダウンロード先となるホームＰＣ１２０に対して、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ)］と、先の（５）の処理において、携帯情報端末１３０から受信した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ)］を送信する。

次に、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ)］と、暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ)］を受信したホームＰＣ１２０は、（９）の処理として、自己の所有する携帯情報端末１３０の公開鍵［Ｋ＿ＰＵＢ２＿ＭＢＬ］を適用して、受信した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ)］の復号処理を実行して、コンテンツ署名用鍵［Ｋｓｉｇ］を取り出して、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ)］の署名検証処理を実行する。この署名検証処理において、コンテンツ（Ｍ）のデータ改竄のないことが立証されたことを条件としてコンテンツの格納または再生処理を実行する。

次に、図１２乃至図１４のフローチャートを参照して、携帯情報端末１３０の

処理、コンテンツ配信サーバ１５０の処理、およびホームＰＣ１２０の処理のそれぞれについて説明する。

まず、図１２のフローチャートを参照して携帯情報端末１３０の処理手順について説明する。ステップＳ３１１において、携帯情報端末１３０は、ダウンロード先となる機器のデバイスチケット、ここではホームＰＣ１２０のホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むデータをコンテンツ配信サーバ１５０に送信して、コンテンツのダウンロードを要求する。

ステップＳ３１２において、携帯情報端末１３０は、コンテンツ配信サーバ１５０の生成したコンテンツ署名用鍵［Ｋｓｉｇ］を受信する。

ステップＳ３１３において、コンテンツ署名用鍵［Ｋｓｉｇ］を受信した携帯情報端末１３０は、携帯情報端末１３０の秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］を適用してコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化して、暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ)］を生成し、ステップＳ３１４において、生成した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ)］をコンテンツ配信サーバ１５０に送信する。

以上の処理が、携帯情報端末１３０とコンテンツ配信サーバ１５０間で実行されるコンテンツダウンロード要求処理における携帯情報端末１３０側の処理である。

次に、図１３を参照して、携帯情報端末１３０からコンテンツダウンロード要求コマンドを受信するコンテンツ配信サーバ１５０の処理について説明する。

まず、コンテンツ配信サーバ１５０は、ステップＳ３２１において、携帯情報端末１３０から、ダウンロード先のデバイスチケット、ここではホームＰＣ１２０のホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むデータをダウンロードコマンドとして受信する。

携帯情報端末１３０からホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むダウンロードコマンドを受信したコンテンツ配信サーバ１５０は、ステップＳ３２２において、ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証処理を実行する。この検証処理は、先に説明したように、ホームＰＣ１２０の公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］の署名（認証局署名）検証による公開鍵証明書［Ｋ＿

ＰＵＢ＿ＨＳ－ｃｅｒｔ］の正当性確認処理、正当性の確認された公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］からのホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］の取得処理、得したホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］を適用したホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，（ＩＤ＿ＨＳ，ＩＤ＿ＭＢＬ，Ｋ＿ＰＵＢ＿ＨＳ））］の署名検証処理を順次行なうことによって実行される。

ステップＳ３２３において、チケット検証が不成立と判定された場合は、チケット、すなわちホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］が偽造されたものである可能性があり、ステップＳ１２９に進み、エラーメッセージを携帯情報端末１３０に送信して処理を終了する。この場合は、コンテンツのダウンロード処理は実行されない、

ステップＳ３２３において、チケット検証が成立したと判定された場合は、ステップＳ３２４に進み、コンテンツ署名用鍵［Ｋｓｉｇ］を生成し、ステップＳ３２５において、生成したコンテンツ署名用鍵［Ｋｓｉｇ］を携帯情報端末１３０に送信する。

次に、コンテンツ配信サーバ１５０は、ステップＳ３２６において、携帯情報端末１３０の秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］を適用してコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ）］を携帯情報端末１３０から受信する。

次に、コンテンツ配信サーバ１５０は、ステップＳ３２７において、先に生成したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、ダウンロード対象のコンテンツ（Ｍ）に対する電子署名を行ない、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ）］を生成する。

次に、コンテンツ配信サーバ１５０は、ステップＳ３２８において、ダウンロード先となるホームＰＣ１２０に対して、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ）］と、先に携帯情報端末１３０から受信した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ）］を送信する。

以上の処理が、携帯情報端末１３０からコンテンツダウンロード要求を受信した配信サーバ１５０の処理である。

次に、図１４を参照して、コンテンツ配信サーバ１５０からコンテンツのダウンロードが実行されるホームＰＣ１２０の処理について説明する。

ホームＰＣ１２０は、ステップＳ３３１において、コンテンツ配信サーバ１５０から、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ)］と、暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ)］を受信する。

ステップＳ３３２において、ホームＰＣ１２０は、自己の所有する携帯情報端末１３０の公開鍵［Ｋ＿ＰＵＢ２＿ＭＢＬ］を適用して、受信した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｋｓｉｇ)］の復号処理を実行する。

ステップＳ３３３において、復号に失敗した場合は、ホームネットエリア共有秘密鍵［Ｋｓｅｃ］が携帯情報端末１３０の有する鍵と異なるなど、正当なホームネットエリア共有秘密鍵でない可能性があり、ステップＳ３３７に進み、受信コンテンツを破棄する。

ステップＳ３３３において、復号に成功した場合は、復号によって取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、署名されたコンテンツデータとしての［Ｓｉｇ（Ｋｓｉｇ，Ｍ)］の署名検証処理を実行する。この署名検証に不成功の場合（Ｓ３３５でＮｏ）は、コンテンツ改竄の可能性があり、ステップＳ３３７に進み、受信コンテンツを破棄する。

署名検証に成功した場合（Ｓ３３５でＹｅｓ）は、ステップＳ３３６において、受信コンテンツをホームＰＣ１２０のストレージに格納し、ダウンロード処理を終了する。

以上の処理が、携帯情報端末１３０からコンテンツダウンロード要求を受信した配信サーバ１５０からのコンテンツを受信し、ダウンロードを実行するホームＰＣ１２０の処理である。

上述したように、本実施例においては、コンテンツ配信サーバ１５０は、携帯情報端末１３０から受信したコンテンツダウンロード先のデバイスチケットの検証が可能となり、携帯情報端末１３０の送付してきたホームＰＣチケットに基づいて、ホームＰＣ１２０が、携帯情報端末１３０の承認しているダウンロード先であることの確認が可能となる。すなわち、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテン

ツダウンロード先のデバイスによる署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホームＰＣが、携帯情報端末の承認しているダウンロード先である確認が可能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。

また、本実施例においては、コンテンツ署名用鍵［Ｋｓｉｇ］を、携帯情報端末１３０の有する携帯情報端末１３０の秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］により暗号化して、携帯情報端末１３０からコンテンツ配信サーバ１５０を介してダウンロード先であるホームＰＣ１２０に送信し、ホームＰＣ１２０において所有する携帯情報端末１３０の公開鍵［Ｋ＿ＰＵＢ２＿ＭＢＬ］により復号してコンテンツ署名用鍵［Ｋｓｉｇ］を取得する構成としたので、先に説明した処理例１，２のようなホームネットエリア共有秘密鍵［Ｋｓｅｃ］を共有することなく、ホームネットエリア内でのみ共有される公開鍵、秘密鍵を所有する構成において、安全なコンテンツダウンロードが実行可能となる。

［コンテンツ配信処理例４］

次に、コンテンツ配信処理例４について説明する。コンテンツ配信処理例４は、コンテンツ配信処理例１，２で適用したホームネットエリア共有秘密鍵［Ｋｓｅｃ］を用いず、一般的な公開鍵方式における公開鍵と秘密鍵の一の鍵を適用した処理を実行する構成例であり、コンテンツ配信サーバ１５０がコンテンツのハッシュ値を算出して、ハッシュ値を携帯情報端末１３０が有する携帯情報端末１３０の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］で暗号化して、携帯情報端末１３０からコンテンツ配信サーバ１５０を介してダウンロード先であるホームＰＣ１２０に送信する処理を実行する構成例である。

図１５乃至図１８を参照して、コンテンツ配信処理例４について説明する。図１５は、コンテンツ配信サーバとコンテンツ配信サーバに対するアクセスを実行する携帯情報端末と、携帯情報端末からの要求に従って、コンテンツをダウンロードする大容量記憶媒体としてのホームストレージを備えたホームＰＣとの３者間で実行する処理を示すシーケンス図である。図１６は携帯情報端末の処理を示

すフローチャート、図１７はコンテンツ配信サーバの処理を示すフローチャート、図１８はホームＰＣの処理を示すフローチャートである。

図１５を参照して、本実施例の処理について説明する。図１５において処理は、図に示す番号（１）～（９）の順に進行する。

まず、（１）の処理として、携帯情報端末１３０は、コンテンツ配信サーバ１５０に対して、コンテンツのダウンロードを要求する。このダウンロード要求には、ダウンロード先となる機器、ここではホームＰＣ１２０から受領したホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］、および、ダウンロード先となるホームＰＣ１２０の公開鍵を格納した公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］が含まれる。ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］は、ホームＰＣ１２０のＩＤ［ＩＤ＿ＨＳ］と、携帯情報端末１３０のＩＤ［ＩＤ＿ＭＢＬ］と、ホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］をメッセージとして、該メッセージにホームＰＣ１２０の秘密鍵［Ｋ＿ＳＥＣ＿ＨＳ］で電子署名をしたデータ、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，（ＩＤ＿ＨＳ，ＩＤ＿ＭＢＬ，Ｋ＿ＰＵＢ＿ＨＳ））］である。

携帯情報端末１３０からホームＰＣチケット［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，（Ｔｉｃｋｅｔ＿ＨＳ））］、ホームＰＣ１２０の公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］を受信したコンテンツ配信サーバ１５０は、携帯情報端末１３０の公開鍵証明書から取得される携帯情報端末１３０の公開鍵を用いて、ホームＰＣチケット［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＭＢＬ，（Ｔｉｃｋｅｔ＿ＨＳ））］の署名検証を実行し、（２）の処理としてホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証処理を実行する。この検証処理の手順は、（ａ）ホームＰＣ１２０の公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］の署名（認証局署名）検証による公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］の正当性確認処理、（ｂ）正当性の確認された公開鍵証明書［Ｋ＿ＰＵＢ＿ＨＳ－ｃｅｒｔ］からのホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］の取得処理、（ｃ）取得したホームＰＣ１２０の公開鍵［Ｋ＿ＰＵＢ＿ＨＳ］を適用したホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］、すなわち、［Ｓｉｇ（Ｋ＿ＳＥＣ＿ＨＳ，（ＩＤ＿ＨＳ，ＩＤ＿ＭＢＬ，Ｋ＿ＰＵＢ＿ＨＳ））］の署名検証処理である。

この手続き、すなわちホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証により、ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］が改竄の無い正当なチケットであることが確認されると、コンテンツ配信サーバ１５０は、（３）の処理として、コンテンツのハッシュ値［Ｈ（Ｍ）］を計算する。次に、（４）の処理として、コンテンツ配信サーバ１５０は、生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を携帯情報端末１３０に送信する。

コンテンツのハッシュ値［Ｈ（Ｍ）］を受信した携帯情報端末１３０は、（５）の処理として、携帯情報端末１３０の第２の秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］を適用してコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化して、暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］を生成し、（６）の処理として、生成した暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］をコンテンツ配信サーバ１５０に送信する。携帯情報端末１３０の第２秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］は、チケットで使用される公開鍵ペアとは別の第２の公開鍵ペアを構成する秘密鍵である。この第２の公開鍵ペアは、ホームネットエリア内のみデ共有される秘密情報である。

（７）の処理として、コンテンツ配信サーバ１５０は、暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］とコンテンツ（Ｍ）からなるコンテンツパッケージ［Ｍ｜Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］を生成し、（８）の処理として、コンテンツ配信サーバ１５０は、ダウンロード先となるホームＰＣ１２０に対して、コンテンツパッケージ［Ｍ｜Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］を送信する。

次に、コンテンツパッケージ［Ｍ｜Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］を受信したホームＰＣ１２０は、（９）の処理として、自己の所有する携帯情報端末１３０の公開鍵［Ｋ＿ＰＵＢ２＿ＭＢＬ］を適用して、受信したコンテンツパッケージ［Ｍ｜Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］に含まれる暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］の復号処理を実行して、コンテンツ署名用鍵［Ｋｓｉｇ］を取り出して、コンテンツのハッシュ値［Ｈ（Ｍ）］を取り出し、また、コンテンツ（Ｍ）に対するハッシュ値を計算して、両ハッシュ値の一致を確認する。一致している場合は、コンテンツの改竄がないと判定し、不一

致の場合は、コンテンツ改竄ありと判定する。検証処理において、コンテンツ（Ｍ）のデータ改竄のないことが立証されたことを条件としてコンテンツの格納または再生処理を実行する。

次に、図１６乃至図１８のフローチャートを参照して、携帯情報端末１３０の処理、コンテンツ配信サーバ１５０の処理、およびホームＰＣ１２０の処理のそれぞれについて説明する。

まず、図１６のフローチャートを参照して携帯情報端末１３０の処理手順について説明する。ステップＳ４１１において、携帯情報端末１３０は、ダウンロード先となる機器のデバイスチケット、ここではホームＰＣ１２０のホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むデータをコンテンツ配信サーバ１５０に送信して、コンテンツのダウンロードを要求する。

ステップＳ４１２において、携帯情報端末１３０は、コンテンツ配信サーバ１５０の生成したコンテンツのハッシュ値［Ｈ（Ｍ)］を受信する。

ステップＳ４１３において、コンテンツのハッシュ値［Ｈ（Ｍ)］を受信した携帯情報端末１３０は、携帯情報端末１３０の第２の秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］を適用してコンテンツのハッシュ値［Ｈ（Ｍ)］を暗号化して、暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ))］を生成し、ステップＳ４１４において、生成した暗号化ハッユ値［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ))］をコンテンツ配信サーバ１５０に送信する。

以上の処理が、携帯情報端末１３０とコンテンツ配信サーバ１５０間で実行されるコンテンツダウンロード要求処理における携帯情報端末１３０側の処理である。

次に、図１７を参照して、携帯情報端末１３０からコンテンツダウンロード要求コマンドを受信するコンテンツ配信サーバ１５０の処理について説明する。

まず、コンテンツ配信サーバ１５０は、ステップＳ４２１において、携帯情報端末１３０から、ダウンロード先のデバイスチケット、ここではホームＰＣ１２０のホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むデータをダウンロードコマンドとして受信する。

携帯情報端末１３０からホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］を含むダ

ウンロードコマンドを受信したコンテンツ配信サーバ１５０は、ステップＳ４２２において、ホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］の検証処理を実行する。この検証処理は、先に説明したと同様の処理である。

ステップＳ４２３において、チケット検証が不成立と判定された場合は、チケット、すなわちホームＰＣチケット［Ｔｉｃｋｅｔ＿ＨＳ］が偽造されたものである可能性があり、ステップＳ４２９に進み、エラーメッセージを携帯情報端末１３０に送信して処理を終了する。この場合は、コンテンツのダウンロード処理は実行されない、

ステップＳ４２３において、チケット検証が成立したと判定された場合は、ステップＳ４２４に進み、コンテンツのハッシュ値［Ｈ（Ｍ）］を生成し、ステップＳ４２５において、生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を携帯情報端末１３０に送信する。

次に、コンテンツ配信サーバ１５０は、ステップＳ４２６において、携帯情報端末１３０の秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］を適用してコンテンツのハッシュ値[Ｈ(Ｍ)]を暗号化した暗号化ハッシュ値[Ｅ(Ｋ＿ＳＥＣ２＿ＭＢＬ,Ｈ(Ｍ))]を携帯情報端末１３０から受信する。

次に、コンテンツ配信サーバ１５０は、ステップＳ４２７において、携帯情報端末１３０から受信した暗号化ハッシュ値[Ｅ(Ｋ＿ＳＥＣ２＿ＭＢＬ,Ｈ(Ｍ))]とコンテンツ（Ｍ）からなるコンテンツパッケージ［Ｍ｜Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］を生成する。

次に、コンテンツ配信サーバ１５０は、ステップＳ４２８において、ダウンロード先となるホームＰＣ１２０に対して、コンテンツパッケージ［Ｍ｜Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］を送信する。

以上の処理が、携帯情報端末１３０からコンテンツダウンロード要求を受信した配信サーバ１５０の処理である。

次に、図１８を参照して、コンテンツ配信サーバ１５０からコンテンツのダウンロードが実行されるホームＰＣ１２０の処理について説明する。

ホームＰＣ１２０は、ステップＳ４３１において、コンテンツ配信サーバ１５０から、コンテンツパッケージ［Ｍ｜Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］を

受信する。

ステップＳ４３２において、ホームＰＣ１２０は、自己の所有する携帯情報端末１３０の公開鍵［Ｋ＿ＰＵＢ２＿ＭＢＬ］を適用して、受信したコンテンツパッケージ［Ｍ｜Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］に含まれる暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ２＿ＭＢＬ，Ｈ（Ｍ））］の復号処理を実行する。

ステップＳ４３３において、復号に失敗した場合は、自己の所有する携帯情報端末１３０の公開鍵［Ｋ＿ＰＵＢ２＿ＭＢＬ］が携帯情報端末１３０の有する秘密鍵に対するペアと異なるなど、正当な公開鍵でない可能性があり、ステップＳ４３７に進み、受信コンテンツを破棄する。

ステップＳ４３３において、復号に成功した場合は、復号によって取得したコンテンツのハッシュ値［Ｈ（Ｍ）］と、コンテンツ（Ｍ）に基づいて計算により算出したハッシュ値Ｈ（Ｍ）’との比較を実行する。この比較において両ハッシュ値が不一致の場合（Ｓ４３５でＮｏ）は、コンテンツ改竄の可能性があり、ステップＳ４３７に進み、受信コンテンツを破棄する。

両ハッシュ値が一致した場合（Ｓ４３５でＹｅｓ）は、ステップＳ４３６において、受信コンテンツをホームＰＣ１２０のストレージに格納し、ダウンロード処理を終了する。

以上の処理が、携帯情報端末１３０からコンテンツダウンロード要求を受信した配信サーバ１５０からのコンテンツを受信し、ダウンロードを実行するホームＰＣ１２０の処理である。

上述したように、本実施例においては、コンテンツ配信サーバ１５０は、携帯情報端末１３０から受信したコンテンツダウンロード先のデバイスチケットの検証が可能となり、携帯情報端末１３０の送付してきたホームＰＣチケットに基づいて、ホームＰＣ１２０が、携帯情報端末１３０の承認しているダウンロード先であることの確認が可能となる。すなわち、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツダウンロード先のデバイスによる署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホームＰＣが、携帯情報端末の承認しているダウンロード先である確認が可

能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。

また、本実施例においては、コンテンツのハッシュ値［Ｈ（Ｍ)］を、携帯情報端末１３０の第２の秘密鍵［Ｋ＿ＳＥＣ２＿ＭＢＬ］により暗号化して、携帯情報端末１３０からコンテンツ配信サーバ１５０を介してダウンロード先であるホームＰＣ１２０に送信し、ホームＰＣ１２０において所有する携帯情報端末１３０の公開鍵[Ｋ＿ＰＵＢ２＿ＭＢＬ]により復号してコンテンツのハッシュ値[Ｈ（Ｍ)]を取得して、コンテンツに基づいてみずから算出するハッシュ値と比較する構成としたので、先に説明した処理例１，２のようなホームネットエリア共有秘密鍵［Ｋｓｅｃ］を共有することなく、ホームネットエリア内でのみ共有される公開鍵、秘密鍵を所有する構成において、安全なコンテンツダウンロードが実行可能となる。

［情報処理装置およびサーバ構成例］

次に本システムを構成するホームＰＣ１２０、携帯情報端末１３０としての情報処理装置、およびコンテンツ配信サーバ１５０の構成例について図１９、図２０を用いて説明する。図１９には、ホームＰＣ１２０、携帯情報端末１３０としての情報処理装置の構成例を示す。

ＣＰＵ(Central processing Unit)５０１は、各種アプリケーションプログラムや、ＯＳ（Operating System）を実行する演算ユニットである。ＲＯＭ（Read-Only-Memory）５０２は、ＣＰＵ５０１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）５０３は、ＣＰＵ５０１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

ホストバス５０４はブリッジ５０５を介してＰＣＩ（Peripheral Component Internet/Interface）バスなどの外部バス５０６に接続されている。

キーボード５０８はＣＰＵ５０１に各種の指令を入力するためにユーザにより操作され、ポインティングデバイス５０９はディスプレイ５１０の画面上の位置

指定、コマンド指定などの際にユーザによって操作される。ディスプレイ５１０は例えばＣＲＴ、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。ＨＤＤ(Hard Disk Drive)５１１は、情報記憶媒体としてのハードディスクを駆動し、ハードディスクからのプログラム、データの読み取りまたはハードディスクに対するプログラム、データの書き込みを実行する。

ドライブ５１２は、フロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体５１３の記録再生を実行するドライブであり、各リムーバブル記録媒体５１３からのプログラムまたはデータ再生、リムーバブル記録媒体５１３に対するプログラムまたはデータ格納を実行する。

各記憶媒体に記録されたプログラムまたはデータを読み出してＣＰＵ５０１において実行または処理を行なう場合は、読み出したプログラム、データはインタフェース５０７、外部バス５０６、ブリッジ５０５、ホストバス５０４を介して例えば接続されているＲＡＭ５０３に供給する。

キーボード５０８乃至ドライブ５１２はインタフェース５０７に接続されており、インタフェース５０７は外部バス５０６、ブリッジ５０５、およびホストバス５０４を介してＣＰＵ５０１に接続されている。

通信部５１４は情報処理装置の接続されたルータ等を介してサーバー装置と通信し、ＣＰＵ５０１、ＨＤＤ５１１等から供給されたデータをパケット化して送信したり、ルータを介してパケットを受信する処理を実行する。通信部５０３は外部バス５０６、ブリッジ５０５、およびホストバス５０４を介してＣＰＵ５０１に接続されている。

次に、コンテンツ配信処理を実行するサーバー装置の構成について図２０を参照して説明する。

ＣＰＵ(Central processing Unit)７０１は、各種アプリケーションプログラムや、ＯＳ（Operating System）を実行する演算ユニットである。ＲＯＭ（Read-Only-Memory）７０２は、ＣＰＵ７０１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）

７０３は、ＣＰＵ７０１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

ドライブ７０５は、フロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体７０６の記録再生を実行するドライブであり、各リムーバブル記録媒体７０６からのプログラムまたはデータ再生、リムーバブル記録媒体７０６に対するプログラムまたはデータ格納を実行する。各記憶媒体に記録されたプログラムまたはデータを読み出してＣＰＵ７０１において実行または処理を行なう場合は、読み出したプログラム、データはバス７０４を介して例えば接続されているＲＡＭ７０３、通信部７０７に供給される。

通信部７０７は、ＰＣ、携帯情報端末等の通信端末との通信部であり、ＣＰＵ７０１のデータ処理によって生成したパケットの送信したり、インターネットを介してパケットを受信する処理を実行する。

ＣＰＵ７０１乃至通信部７０７はバス７０４によって相互接続され、データの転送が可能な構成となっている。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only

Memory)に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

産業上の利用可能性

以上説明してきたように、本発明の構成によれば、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツダウンロード先の装置による署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホームＰＣが、携帯情報端末の承認しているダウンロード先である確認が可能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。

また、本発明の一実施例構成によれば、コンテンツ署名用鍵［Ｋｓｉｇ］を、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置と、コンテンツダウンロード先としての情報処理装置、例えばホームＰＣとの共有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］により暗号化して、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツ配

信サーバを介してダウンロード先である情報処理装置、例えばホームＰＣに送信し、ホームＰＣにおいて所有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］により復号してコンテンツ署名用鍵［Ｋｓｉｇ］を取得する構成としたので、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置と、コンテンツダウンロード先としての情報処理装置、例えばホームＰＣとが同一のホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有することが、ダウンロード先であるホームＰＣにおいてコンテンツ署名用鍵［Ｋｓｉｇ］を取得できる条件となり、同一のホームネットエリア共有秘密鍵[Ｋｓｅｃ]を有する機器間においてのみ、有効なコンテンツの検証、ダウンロードが実行可能となり、不正コンテンツの格納を防止することが可能となる。

また、本発明の一実施例構成によれば、コンテンツのハッシュ値[Ｈ(Ｍ)]を、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置と、コンテンツダウンロード先としての情報処理装置、例えばホームＰＣとが共有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］により暗号化して、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置から、コンテンツ配信サーバを介して、コンテンツダウンロード先としての情報処理装置、例えばホームＰＣに送信し、ホームＰＣにおいて所有するホームネットエリア共有秘密鍵［Ｋｓｅｃ］により復号してコンテンツのハッシュ値［Ｈ（Ｍ)］を取得して、コンテンツに基づいてみずから算出するハッシュ値と比較する構成としたので、同一のホームネットエリア共有秘密鍵[Ｋｓｅｃ]を有する機器間においてのみ、有効なコンテンツの検証、ダウンロードが実行可能となり、不正コンテンツの格納を防止することが可能となる。

また、本発明の一実施例構成によれば、コンテンツ署名用鍵［Ｋｓｉｇ]、あるいはコンテンツのハッシュ値［Ｈ（Ｍ)］を、コンテンツダウンロード要求を行なう例えば携帯情報端末の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］により暗号化して、携帯情報端末からコンテンツ配信サーバを介してダウンロード先であるホームＰＣに送信し、ホームＰＣにおいて所有する携帯情報端末の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］により復号してコンテンツ署名用鍵［Ｋｓｉｇ]、あるいはコンテンツのハッシュ値［Ｈ（Ｍ)］を取得して、コンテンツの検証を実行する構成としたので、ホ

ームネットエリア共有秘密鍵［Ｋｓｅｃ］を共有することなく、通常の公開鍵方式の公開鍵、秘密鍵を所有する構成において、セキュアなコンテンツダウンロード処理が実行可能となる。

請求の範囲

１．　自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行
する第１の情報処理装置と、
コンテンツのダウンロード先として指定される第２の情報処理装置と、
前記第１の情報処理装置からのコンテンツダウンロード要求を受信して、前記第２の情報処理装置に対するコンテンツの送信処理を実行するコンテンツ配信サーバとを有し、
前記第１の情報処理装置は、
前記第２の情報処理装置の電子署名がなされたチケットを前記コンテンツ配信サーバに送信する処理を実行し、
前記コンテンツ配信サーバは、
前記チケットの電子署名の検証を実行し、該検証に成功したことを条件として、前記第２の情報処理装置が前記第１の情報処理装置の承認したコンテンツダウンロード先であると判定して、前記第２の情報処理装置に対するコンテンツ送信を実行する構成を有することを特徴とするコンテンツ配信システム。

２．　前記第１の情報処理装置と、前記第２の情報処理装置は、共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有し、
前記第１の情報処理装置は、
前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、
前記第２の情報処理装置は、
前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］による暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］の復号により取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行する構

成であることを特徴とする請求項１に記載のコンテンツ配信システム。

３．　前記第１の情報処理装置と、前記第２の情報処理装置は、共有する秘密鍵とし
てのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を有し、

前記第１の情報処理装置は、

前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、

前記第２の情報処理装置は、

前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］による暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］の復号により取得したコンテンツのハッシュ値［Ｈ（Ｍ）］を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行する構成であることを特徴とする請求項１に記載のコンテンツ配信システム。

４．　前記第１の情報処理装置と、前記第２の情報処理装置は、それぞれ公開鍵暗号方式の公開鍵、秘密鍵を有し、

前記第１の情報処理装置は、

該第１の情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｋｓｉｇ）］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、

前記第２の情報処理装置は、

前記第１の情報処理装置の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］による暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｋｓｉｇ）］の復号により取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行する構成であることを特徴とする請求項１に記載のコンテンツ配信システム。

５．　前記第１の情報処理装置と、前記第２の情報処理装置は、それぞれ公開鍵暗号方式の公開鍵、秘密鍵を有し、

前記第１の情報処理装置は、

該第１の情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、

前記第２の情報処理装置は、

前記第１の情報処理装置の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］による暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］の復号により取得したコンテンツのハッシュ値［Ｈ（Ｍ）］を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行する構成であることを特徴とする請求項１に記載のコンテンツ配信システム。

６．　前記チケットは、前記第１の情報処理装置と、前記第２の情報処理装置各々の識別子（ＩＤ）を含むデータに対して、前記第２の情報処理装置の秘密鍵による電子署名がなされたチケットであり、

前記コンテンツ配信サーバは、

前記第２の情報処理装置の公開鍵を適用して、前記チケットの電子署名の検証を実行する構成であることを特徴とする請求項１に記載のコンテンツ配信システム。

７．　前記コンテンツ配信サーバは、

前記チケットの電子署名の検証処理として、以下の処理

（ａ）前記第２の情報処理装置の公開鍵証明書の署名（認証局署名）検証による公開鍵証明書の正当性確認処理、

（ｂ）正当性の確認された公開鍵証明書からの前記第２の情報処理装置の公開鍵の取得処理、

（ｃ）取得した前記第２の情報処理装置の公開鍵を適用した前記第２の情報処理装置のチケットの署名検証処理、

の各処理を実行する構成であることを特徴とする請求項１に記載のコンテンツ配信システム。

８．　自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行する第１の情報処理装置と、コンテンツのダウンロード先として指定される第２の情報処理装置と、前記第１の情報処理装置からのコンテンツダウンロード要求を受信して、前記第２の情報処理装置に対するコンテンツの送信処理を実行するコンテンツ配信サーバとを有するコンテンツ配信システムにおけるコンテンツ配信方法であり、

前記第１の情報処理装置において、

前記第２の情報処理装置の電子署名がなされたチケットを前記コンテンツ配信サーバに送信するステップと、

前記コンテンツ配信サーバにおいて、

前記チケットの電子署名の検証を実行するステップと、

前記検証に成功したことを条件として、前記第２の情報処理装置が前記第１の情報処理装置の承認したコンテンツダウンロード先であると判定して、前記第２の情報処理装置に対するコンテンツ送信を実行するステップと、

を有することを特徴とするコンテンツ配信方法。

９．　前記コンテンツ配信方法において、

前記第１の情報処理装置は、

前記第１の情報処理装置と、前記第２の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、

前記第２の情報処理装置は、

前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］による暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］の復号により取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行することを特徴とする請求項８に記載のコンテンツ配信方法。

１０．　前記コンテンツ配信方法において、

前記第１の情報処理装置は、

前記第１の情報処理装置と、前記第２の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、

前記第２の情報処理装置は、

前記ホームネットエリア共有秘密鍵［Ｋｓｅｃ］による暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］の復号により取得したコンテンツのハッシュ値［Ｈ（Ｍ）］を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行することを特徴とする請求項８に記載のコンテンツ配信方法。

１１．　前記コンテンツ配信方法において、

前記第１の情報処理装置は、

該第１の情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｋｓｉｇ）］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、

前記第２の情報処理装置は、

前記第１の情報処理装置の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］による暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｋｓｉｇ）］の復号により取得したコンテンツ署名用鍵［Ｋｓｉｇ］を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行することを特徴とする請求項８に記載のコンテンツ配信方法。

１２．　前記コンテンツ配信方法において、

前記第１の情報処理装置は、

該第１の情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］を、コンテンツ配信サーバを介して第２の情報処理装置に送信する処理を実行し、

前記第２の情報処理装置は、

前記第１の情報処理装置の公開鍵［Ｋ＿ＰＵＢ＿ＭＢＬ］による暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］の復号により取得したコンテンツのハッシュ値［Ｈ（Ｍ）］を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行することを特徴とする請求項８に記載のコンテンツ配信方法。

１３．　前記チケットは、前記第１の情報処理装置と、前記第２の情報処理装置各々の識別子（ＩＤ）を含むデータに対して、前記第２の情報処理装置の秘密鍵による電子署名がなされたチケットであり、

前記コンテンツ配信サーバは、

前記第２の情報処理装置の公開鍵を適用して、前記チケットの電子署名の検証を実行することを特徴とする請求項８に記載のコンテンツ配信方法。

１４．　前記コンテンツ配信サーバは、

前記チケットの電子署名の検証処理として、

（ａ）前記第２の情報処理装置の公開鍵証明書の署名（認証局署名）検証による公開鍵証明書の正当性確認処理、

（ｂ）正当性の確認された公開鍵証明書からの前記第２の情報処理装置の公開鍵の取得処理、

（ｃ）取得した前記第２の情報処理装置の公開鍵を適用した前記第２の情報処理装置のチケットの署名検証処理、

の各処理を実行することを特徴とする請求項８に記載のコンテンツ配信方法。

１５．　自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行する情報処理装置であり、

コンテンツのダウンロード先の第２の情報処理装置の電子署名がなされたチケットを格納した記憶手段と、

前記記憶手段に格納した前記チケットを含むコンテンツダウンロード要求コマンドを生成する制御手段と、

前記チケットを含むコンテンツダウンロード要求コマンドをコンテンツ配信サーバに対して送信する通信手段と、

を有することを特徴とする情報処理装置。

１６．　前記情報処理装置の制御手段は、

該情報処理装置と、前記第２の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋｓｅｃ，Ｋｓｉｇ）］を、前記第２の情報処理装置に対する送信データとして生成する構成を有することを特徴とする請求項１５に記載の情報処理装置。

１７．　前記情報処理装置の制御手段は、

該情報処理装置と、前記第２の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵［Ｋｓｅｃ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋｓｅｃ，Ｈ（Ｍ））］を、前記第２の情報処理装置に対する送信データとして生成する構成を有することを特徴とする請求項１５に記載の情報処理装置。

１８．　前記情報処理装置の制御手段は、

該情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵［Ｋｓｉｇ］を暗号化した暗号化鍵データ［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｋｓｉｇ）］を、前記第２の情報処理装置に対

する送信データとして生成する構成を有することを特徴とする請求項１５に記載の情報処理装置。

１９．　前記情報処理装置の制御手段は、

該情報処理装置の秘密鍵［Ｋ＿ＳＥＣ＿ＭＢＬ］を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値［Ｈ（Ｍ）］を暗号化した暗号化ハッシュ値［Ｅ（Ｋ＿ＳＥＣ＿ＭＢＬ，Ｈ（Ｍ））］を、前記第２の情報処理装置に対する送信データとして生成する構成を有することを特徴とする請求項１５に記載の情報処理装置。

２０．　自装置と異なるダウンロード先を指定したコンテンツダウンロード要求処理を実行するコンピュータ・プログラムであり、

コンテンツのダウンロード先の第２の情報処理装置の電子署名がなされたチケットを取得するステップと、

前記チケットを含むコンテンツダウンロード要求コマンドを生成するステップと、

前記チケットを含むコンテンツダウンロード要求コマンドをコンテンツ配信サーバに対して送信するステップと、

を有することを特徴とするコンピュータ・プログラム。

２１．　コンテンツの送信処理を実行するコンピュータ・プログラムであり、

第１の情報処理装置から自装置と異なるダウンロード先として第２の情報処理装置を指定したコンテンツダウンロード要求処理を受信するステップと、

前記コンテンツダウンロード要求に含まれるダウンロード先の第２の情報処理装置の電子署名がなされたチケットに含まれる電子署名検証処理を実行するステップと、

前記検証に成功したことを条件として、前記第２の情報処理装置に対するコンテンツ送信を実行するステップと、

を有することを特徴とするコンピュータ・プログラム。

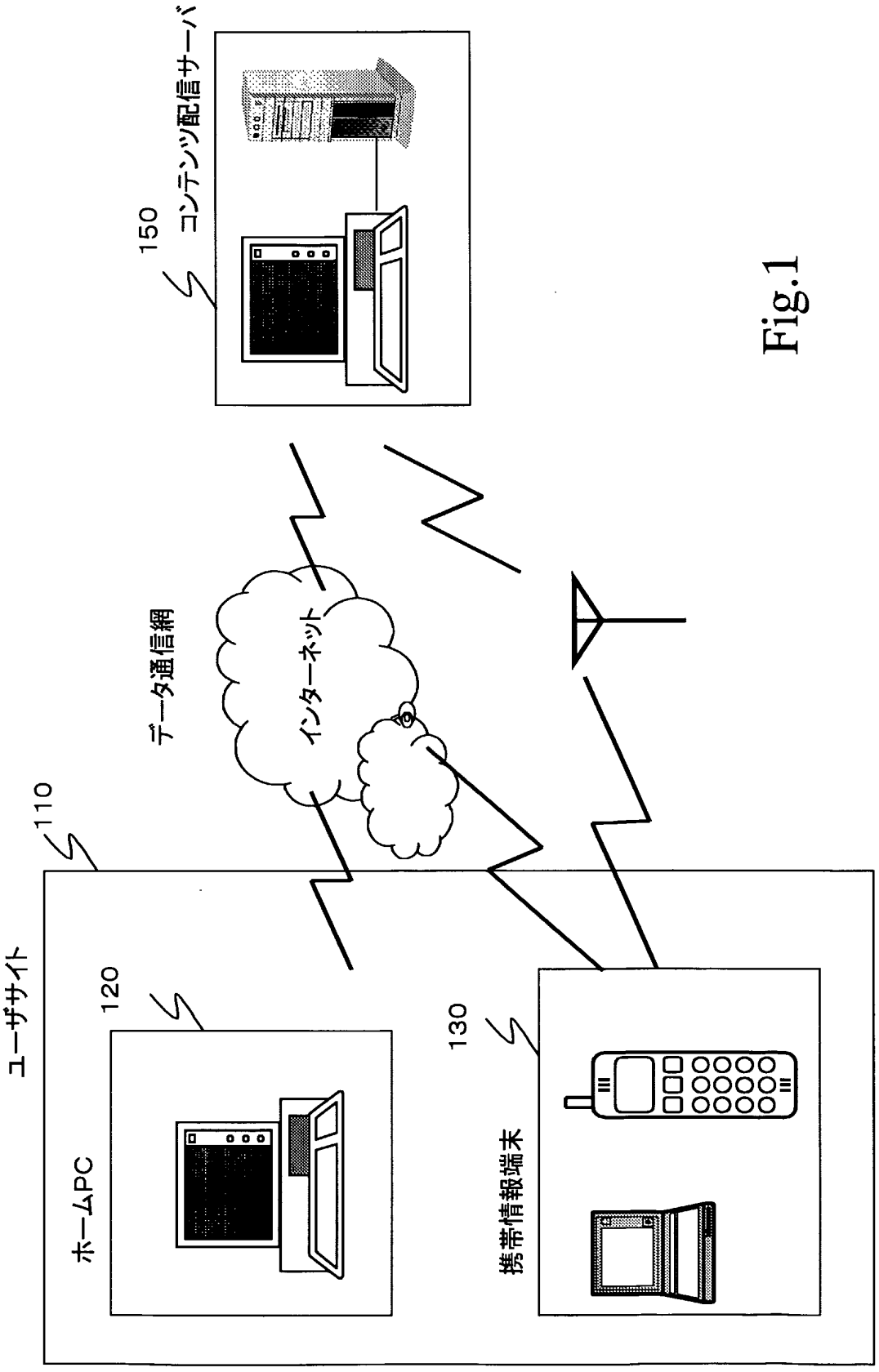

150
コンテンツ配信サーバ
データ通信網
インターネット
110
ユーザサイト
120
ホームPC
130
携帯情報端末

Fig.1

Fig.2

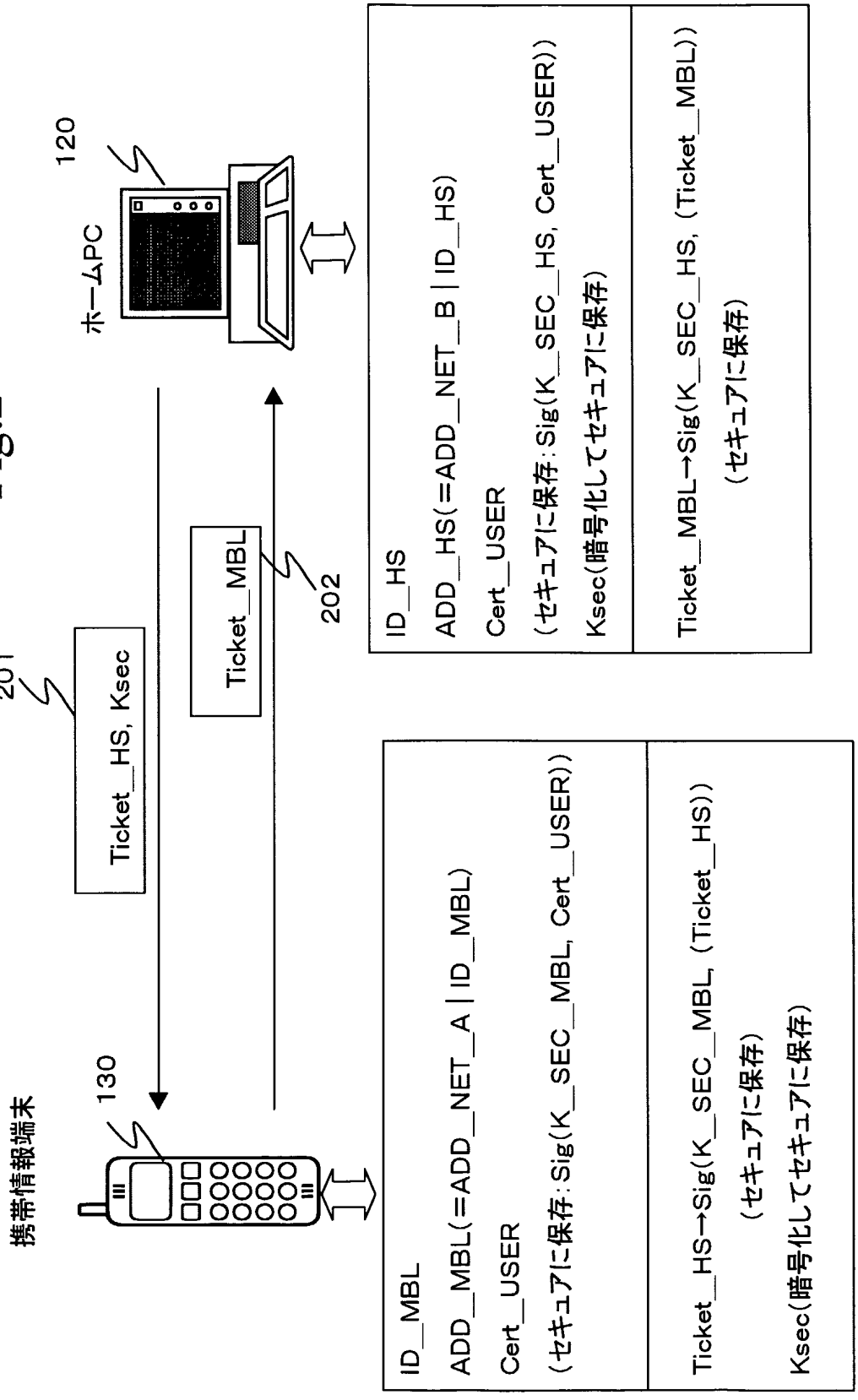
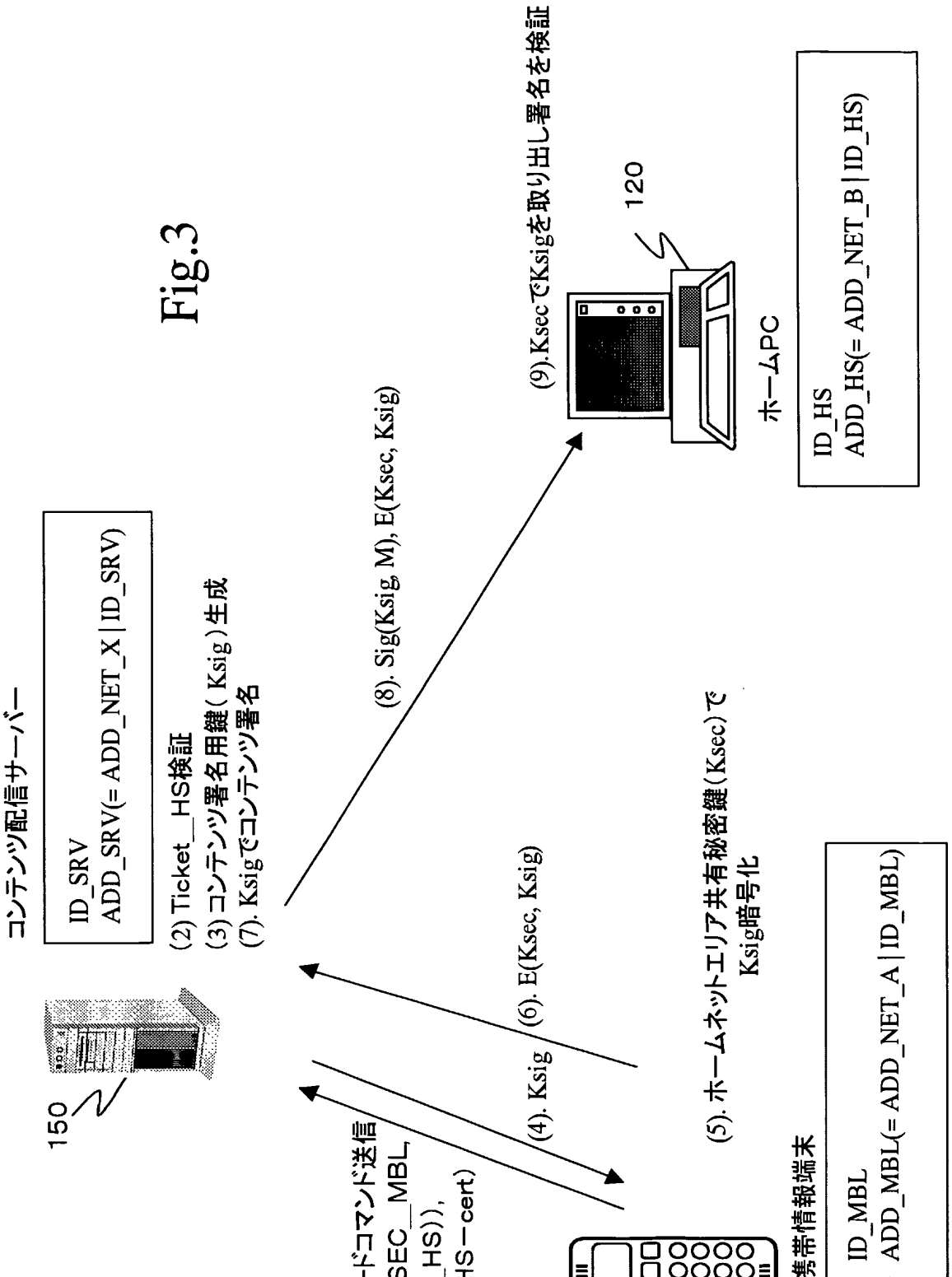

携帯情報端末
130
ホームPC
120
201
Ticket_HS, Ksec
Ticket_MBL
202
ID_MBL
ADD_MBL(=ADD_NET_A | ID_MBL)
Cert_USER
(セキュアに保存:Sig(K_SEC_MBL, Cert_USER))
Ticket_HS→Sig(K_SEC_MBL, (Ticket_HS))
(セキュアに保存)
Ksec(暗号化してセキュアに保存)
ID_HS
ADD_HS(=ADD_NET_B | ID_HS)
Cert_USER
(セキュアに保存:Sig(K_SEC_HS, Cert_USER))
Ksec(暗号化してセキュアに保存)
Ticket_MBL→Sig(K_SEC_HS, (Ticket_MBL))
(セキュアに保存)

Fig.3


コンテンツ配信サーバー
ID_SRV
ADD_SRV(= ADD_NET_X | ID_SRV)
150
(1) ダウンロードコマンド送信
(Sig(K_SEC_MBL
(Ticket_HS)),
K_PUB_HS−cert)
(2) Ticket_HS検証
(3) コンテンツ署名用鍵(Ksig)生成
(7). Ksigでコンテンツ署名
(4). Ksig
(6). E(Ksec, Ksig)
(8). Sig(Ksig, M), E(Ksec, Ksig)
(9).KsecでKsigを取り出し署名を検証
(5). ホームネットエリア共有秘密鍵(Ksec)で
Ksig暗号化
120
ホームPC
ID_HS
ADD_HS(= ADD_NET_B | ID_HS)
130
携帯情報端末
ID_MBL
ADD_MBL(= ADD_NET_A | ID_MBL)

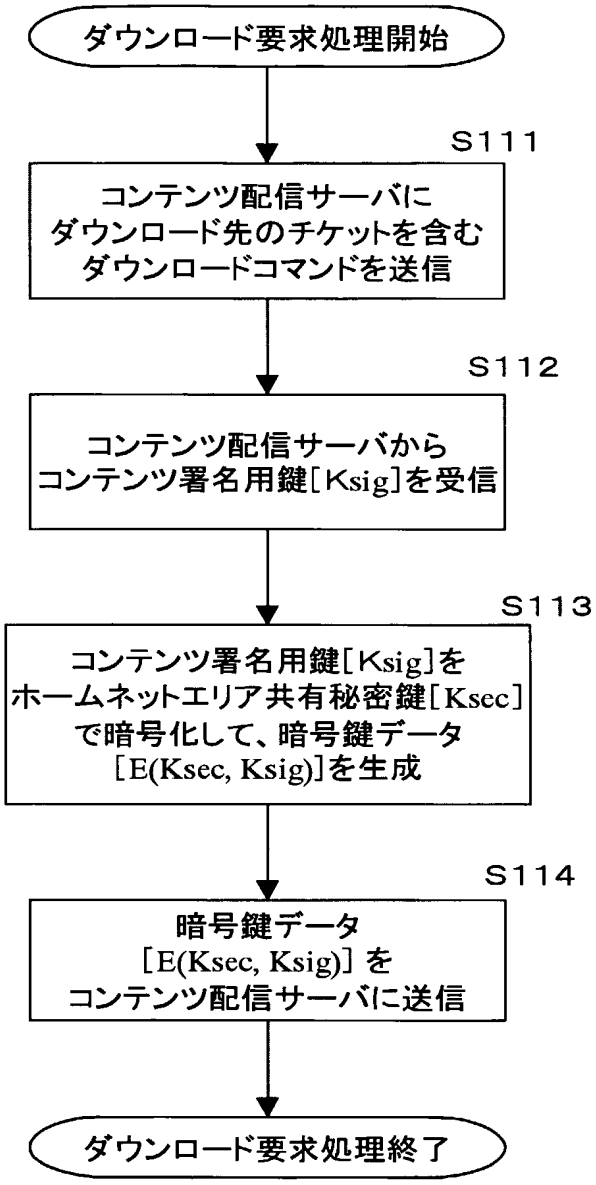

ダウンロード要求処理開始
S111
コンテンツ配信サーバに
ダウンロード先のチケットを含む
ダウンロードコマンドを送信
S112
コンテンツ配信サーバから
コンテンツ署名用鍵[Ksig]を受信
S113
コンテンツ署名用鍵[Ksig]を
ホームネットエリア共有秘密鍵[Ksec]
で暗号化して、暗号鍵データ
[E(Ksec, Ksig)]を生成
S114
暗号鍵データ
[E(Ksec, Ksig)] を
コンテンツ配信サーバに送信
ダウンロード要求処理終了

Fig.4

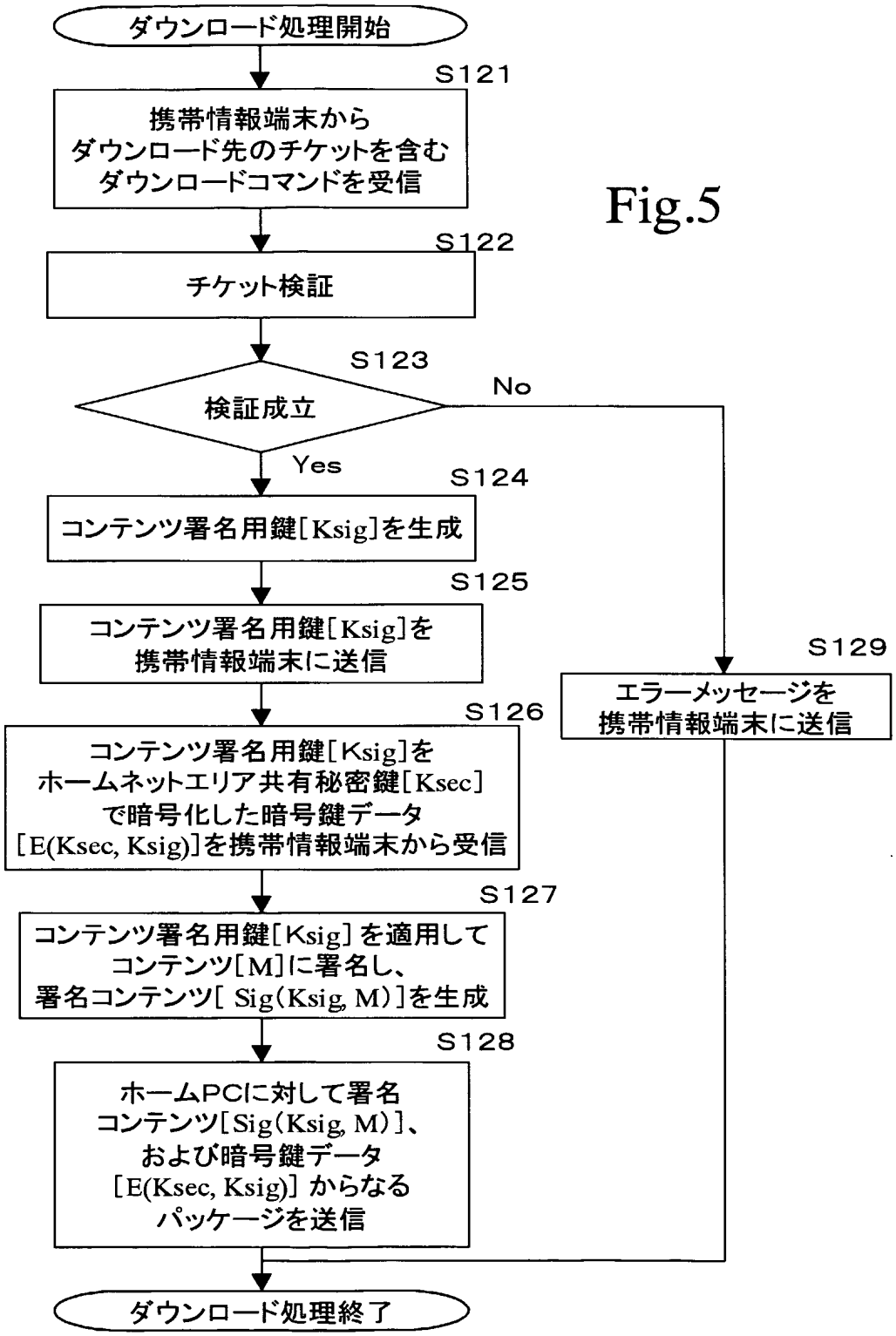

ダウンロード処理開始
S121
携帯情報端末から
ダウンロード先のチケットを含む
ダウンロードコマンドを受信
S122
チケット検証
S123
検証成立
No
Yes
S124
コンテンツ署名用鍵[Ksig]を生成
S125
コンテンツ署名用鍵[Ksig]を
携帯情報端末に送信
S129
エラーメッセージを
携帯情報端末に送信
S126
コンテンツ署名用鍵[Ksig]を
ホームネットエリア共有秘密鍵[Ksec]
で暗号化した暗号鍵データ
[E(Ksec, Ksig)]を携帯情報端末から受信
S127
コンテンツ署名用鍵[Ksig]を適用して
コンテンツ[M]に署名し、
署名コンテンツ[Sig(Ksig, M)]を生成
S128
ホームPCに対して署名
コンテンツ[Sig(Ksig, M)]、
および暗号鍵データ
[E(Ksec, Ksig)] からなる
パッケージを送信
ダウンロード処理終了

Fig.5

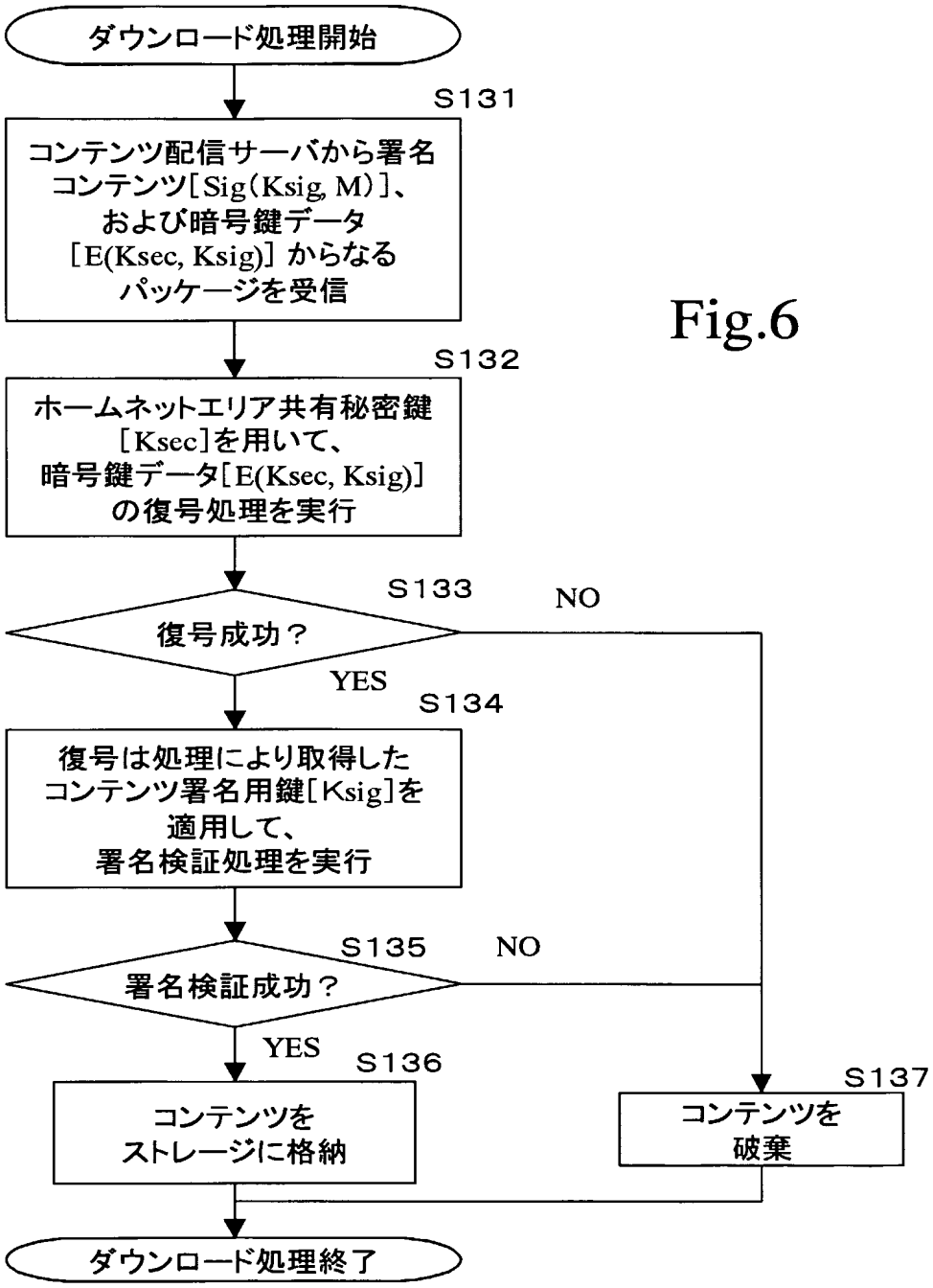

ダウンロード処理開始
S131
コンテンツ配信サーバから署名コンテンツ[Sig(Ksig, M)]、および暗号鍵データ[E(Ksec, Ksig)]からなるパッケージを受信
S132
ホームネットエリア共有秘密鍵[Ksec]を用いて、暗号鍵データ[E(Ksec, Ksig)]の復号処理を実行
S133
復号成功？
NO
YES
S134
復号は処理により取得したコンテンツ署名用鍵[Ksig]を適用して、署名検証処理を実行
S135
署名検証成功？
NO
YES
S136
コンテンツをストレージに格納
S137
コンテンツを破棄
ダウンロード処理終了

Fig.6

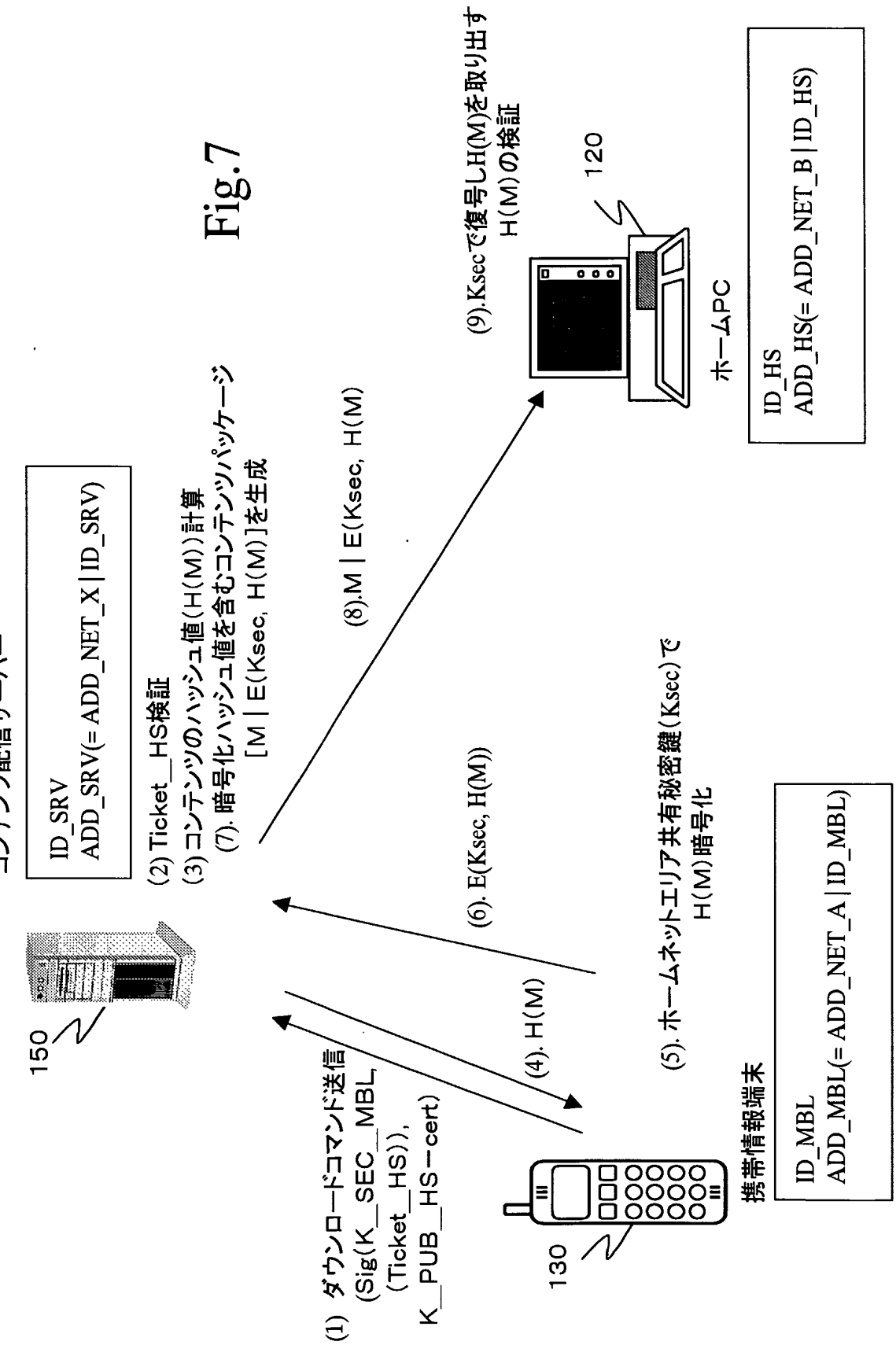

コンテンツ配信サーバー
ID_SRV
ADD_SRV(= ADD_NET_X | ID_SRV)
150
(1) ダウンロードコマンド送信
(Sig(K_SEC_MBL
(Ticket_HS)),
K_PUB_HS−cert)
(2) Ticket_HS検証
(3) コンテンツのハッシュ値(H(M))計算
(7). 暗号化ハッシュ値を含むコンテンツパッケージ
[M | E(Ksec, H(M)]を生成
(4). H(M)
(6). E(Ksec, H(M))
(8).M | E(Ksec, H(M)
(5). ホームネットエリア共有秘密鍵(Ksec)で
H(M)暗号化
(9).Ksecで復号しH(M)を取り出す
H(M)の検証
120
ホームPC
ID_HS
ADD_HS(= ADD_NET_B | ID_HS)
130
携帯情報端末
ID_MBL
ADD_MBL(= ADD_NET_A | ID_MBL)

Fig.7

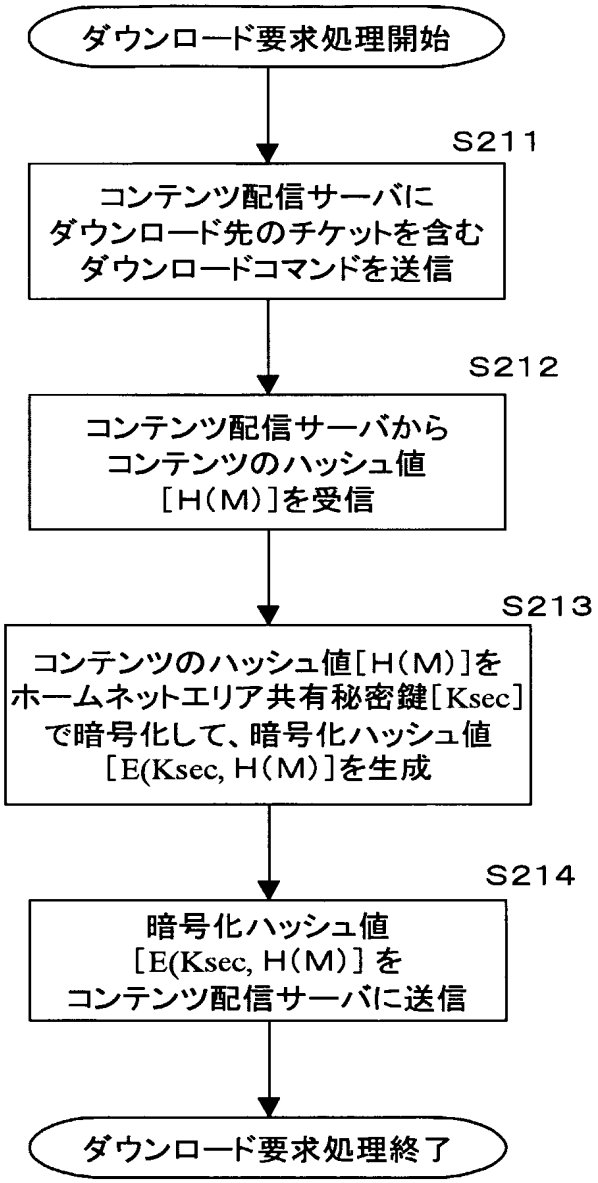

ダウンロード要求処理開始
S211
コンテンツ配信サーバに
ダウンロード先のチケットを含む
ダウンロードコマンドを送信
S212
コンテンツ配信サーバから
コンテンツのハッシュ値
[H(M)]を受信
S213
コンテンツのハッシュ値[H(M)]を
ホームネットエリア共有秘密鍵[Ksec]
で暗号化して、暗号化ハッシュ値
[E(Ksec, H(M)]を生成
S214
暗号化ハッシュ値
[E(Ksec, H(M)] を
コンテンツ配信サーバに送信
ダウンロード要求処理終了

Fig.8

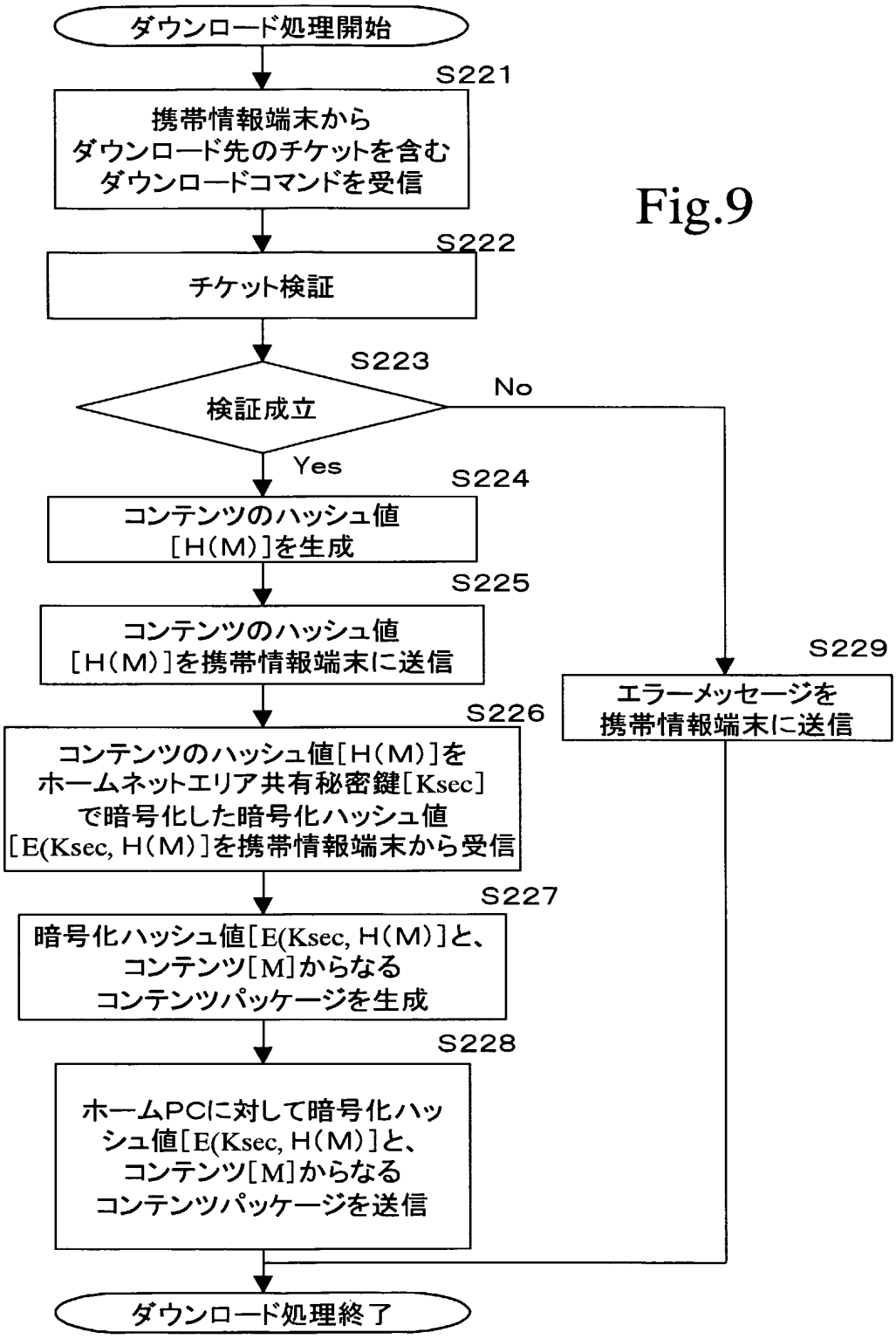

ダウンロード処理開始
S221
携帯情報端末から
ダウンロード先のチケットを含む
ダウンロードコマンドを受信
S222
チケット検証
S223
検証成立
No
Yes
S224
コンテンツのハッシュ値
[H(M)]を生成
S225
コンテンツのハッシュ値
[H(M)]を携帯情報端末に送信
S226
コンテンツのハッシュ値[H(M)]を
ホームネットエリア共有秘密鍵[Ksec]
で暗号化した暗号化ハッシュ値
[E(Ksec, H(M)]を携帯情報端末から受信
S227
暗号化ハッシュ値[E(Ksec, H(M)]と、
コンテンツ[M]からなる
コンテンツパッケージを生成
S228
ホームPCに対して暗号化ハッ
シュ値[E(Ksec, H(M)]と、
コンテンツ[M]からなる
コンテンツパッケージを送信
S229
エラーメッセージを
携帯情報端末に送信
ダウンロード処理終了

Fig.9

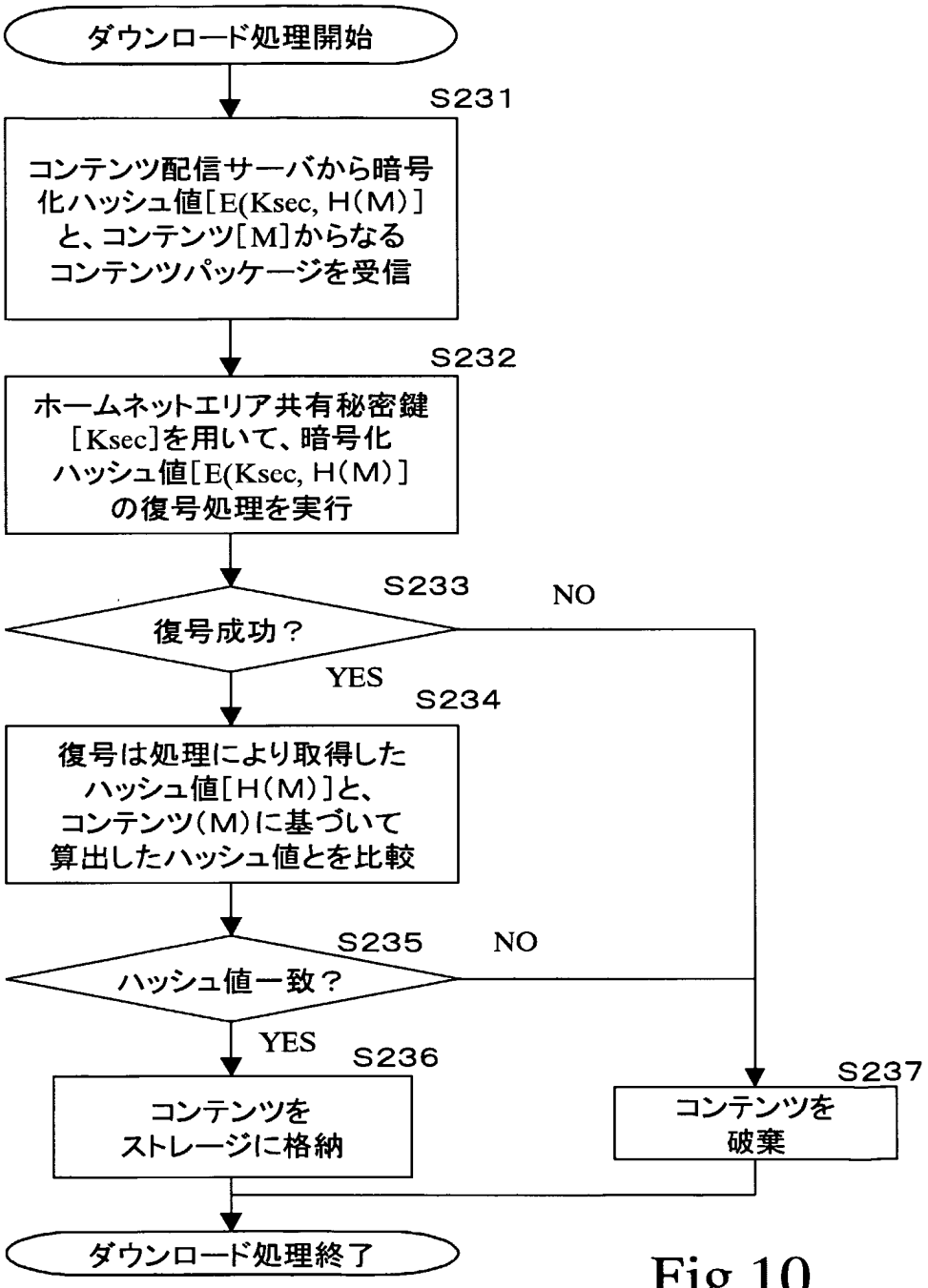
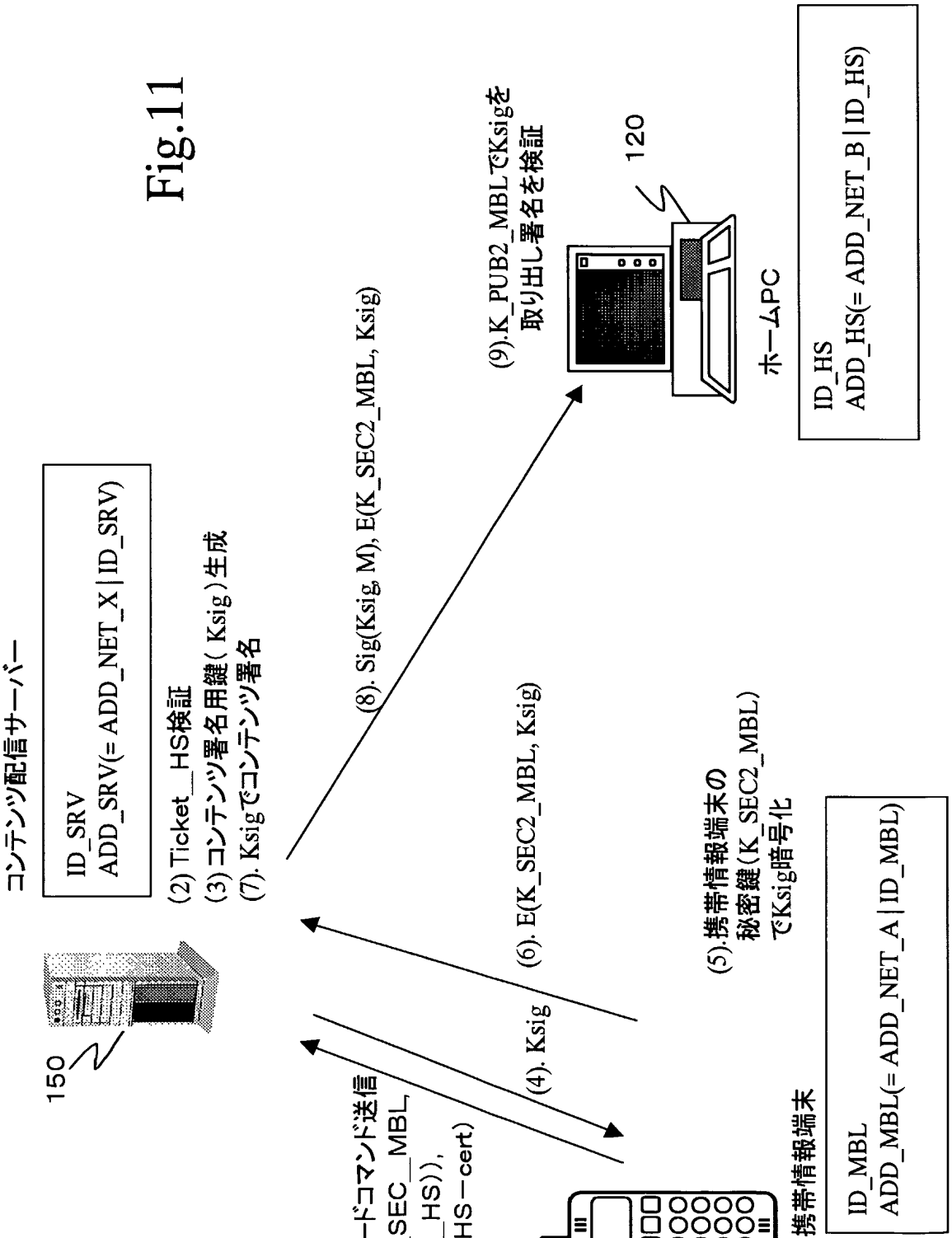

ダウンロード処理開始
S231
コンテンツ配信サーバから暗号化ハッシュ値[E(Ksec, H(M)]と、コンテンツ[M]からなるコンテンツパッケージを受信
S232
ホームネットエリア共有秘密鍵[Ksec]を用いて、暗号化ハッシュ値[E(Ksec, H(M)]の復号処理を実行
S233
復号成功？
NO
YES
S234
復号は処理により取得したハッシュ値[H(M)]と、コンテンツ(M)に基づいて算出したハッシュ値とを比較
S235
ハッシュ値一致？
NO
YES
S236
コンテンツをストレージに格納
S237
コンテンツを破棄
ダウンロード処理終了

Fig.10

Fig.11


コンテンツ配信サーバー
ID_SRV
ADD_SRV(= ADD_NET_X | ID_SRV)
150
(1) ダウンロードコマンド送信
(Sig(K_SEC_MBL
(Ticket_HS)),
K_PUB_HS−cert)
(2) Ticket_HS検証
(3) コンテンツ署名用鍵(Ksig)生成
(7). Ksigでコンテンツ署名
(8). Sig(Ksig, M), E(K_SEC2_MBL, Ksig)
(9).K_PUB2_MBLでKsigを
取り出し署名を検証
120
ホームPC
ID_HS
ADD_HS(= ADD_NET_B | ID_HS)
(6). E(K_SEC2_MBL, Ksig)
(4). Ksig
(5).携帯情報端末の
秘密鍵(K_SEC2_MBL)
でKsig暗号化
130
携帯情報端末
ID_MBL
ADD_MBL(= ADD_NET_A | ID_MBL)

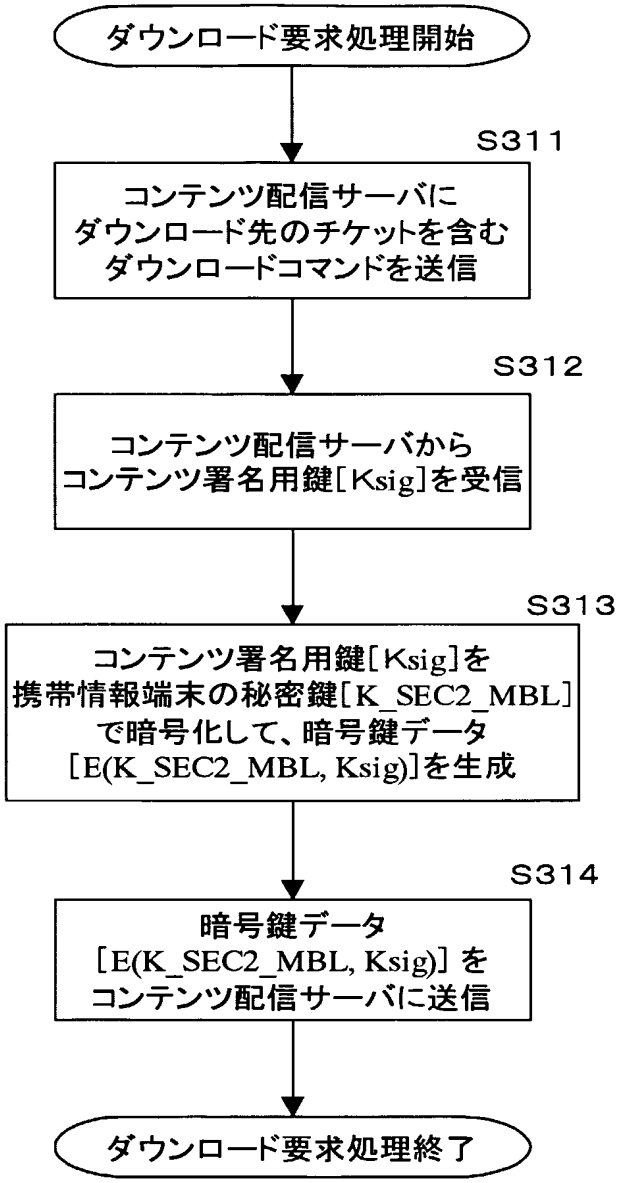

ダウンロード要求処理開始
S311
コンテンツ配信サーバに
ダウンロード先のチケットを含む
ダウンロードコマンドを送信
S312
コンテンツ配信サーバから
コンテンツ署名用鍵[Ksig]を受信
S313
コンテンツ署名用鍵[Ksig]を
携帯情報端末の秘密鍵[K_SEC2_MBL]
で暗号化して、暗号鍵データ
[E(K_SEC2_MBL, Ksig)]を生成
S314
暗号鍵データ
[E(K_SEC2_MBL, Ksig)] を
コンテンツ配信サーバに送信
ダウンロード要求処理終了

Fig.12

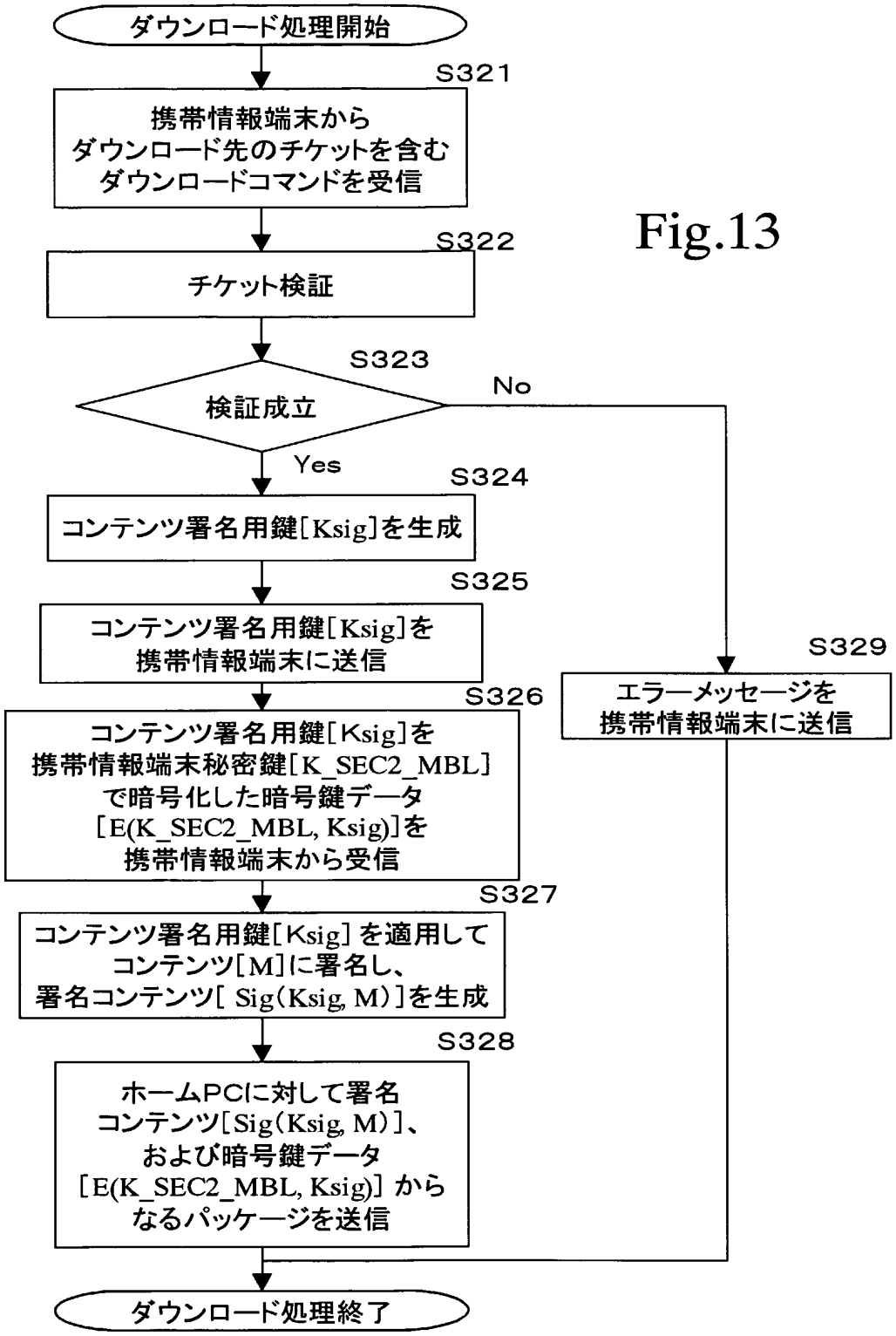

ダウンロード処理開始
S321
携帯情報端末から
ダウンロード先のチケットを含む
ダウンロードコマンドを受信
S322
チケット検証
S323
検証成立
No
Yes
S324
コンテンツ署名用鍵[Ksig]を生成
S325
コンテンツ署名用鍵[Ksig]を
携帯情報端末に送信
S326
コンテンツ署名用鍵[Ksig]を
携帯情報端末秘密鍵[K_SEC2_MBL]
で暗号化した暗号鍵データ
[E(K_SEC2_MBL, Ksig)]を
携帯情報端末から受信
S327
コンテンツ署名用鍵[Ksig] を適用して
コンテンツ[M]に署名し、
署名コンテンツ[Sig(Ksig, M)]を生成
S328
ホームPCに対して署名
コンテンツ[Sig(Ksig, M)]、
および暗号鍵データ
[E(K_SEC2_MBL, Ksig)] から
なるパッケージを送信
S329
エラーメッセージを
携帯情報端末に送信
ダウンロード処理終了

Fig.13

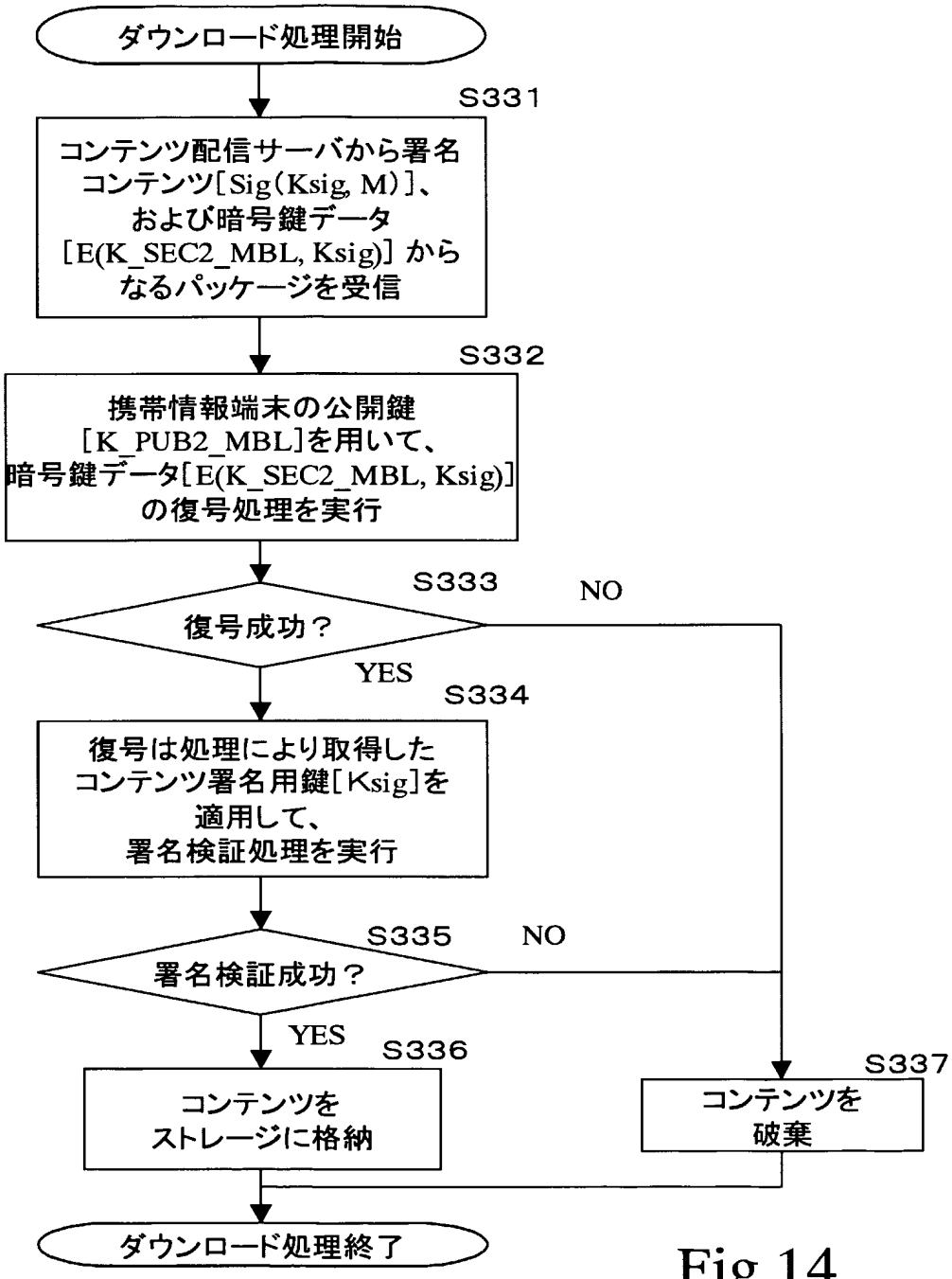
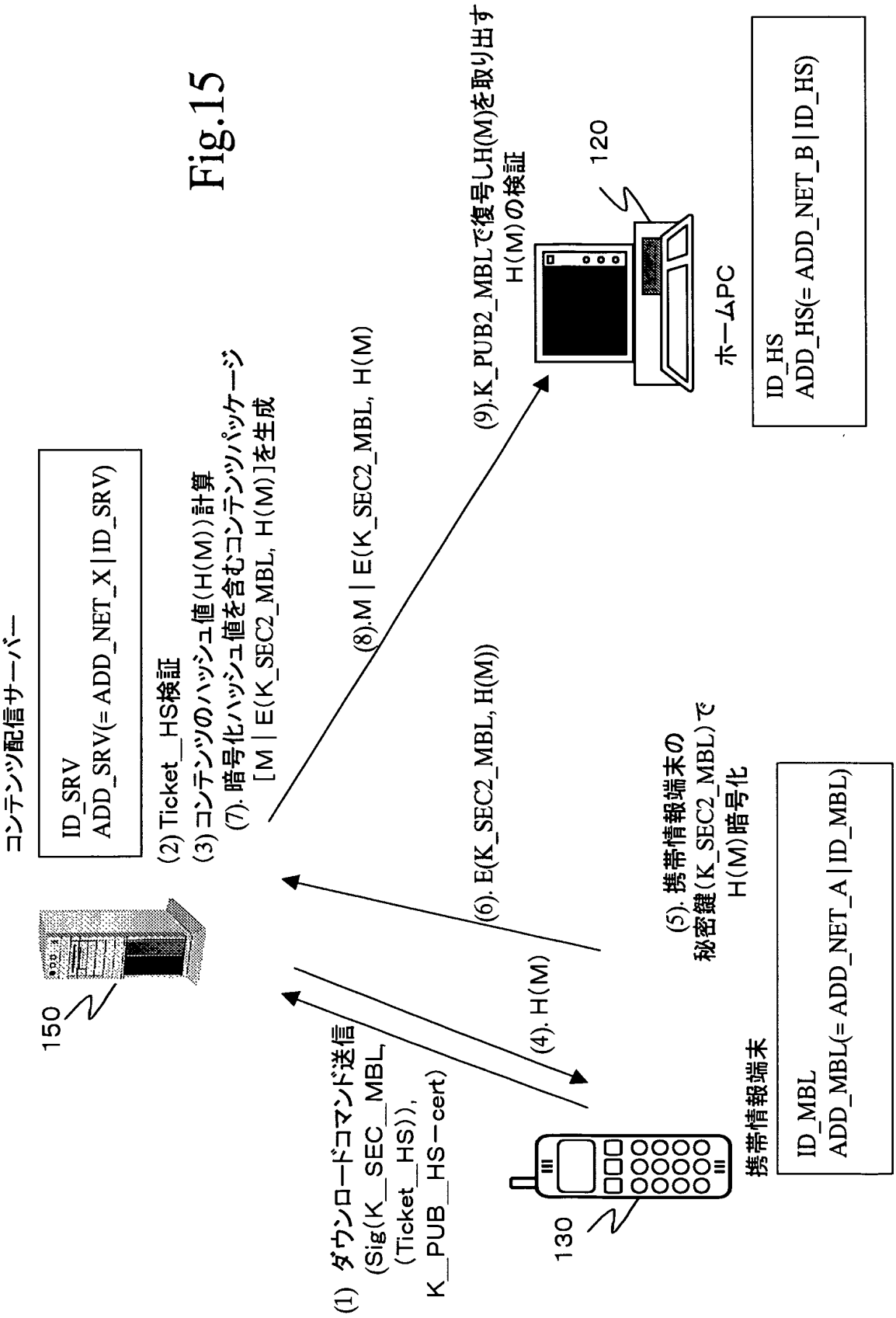

ダウンロード処理開始
S331
コンテンツ配信サーバから署名コンテンツ[Sig(Ksig, M)]、および暗号鍵データ[E(K_SEC2_MBL, Ksig)]からなるパッケージを受信
S332
携帯情報端末の公開鍵[K_PUB2_MBL]を用いて、暗号鍵データ[E(K_SEC2_MBL, Ksig)]の復号処理を実行
S333
復号成功？
NO
YES
S334
復号は処理により取得したコンテンツ署名用鍵[Ksig]を適用して、署名検証処理を実行
S335
署名検証成功？
NO
YES
S336
コンテンツをストレージに格納
S337
コンテンツを破棄
ダウンロード処理終了

Fig.14

Fig.15


コンテンツ配信サーバー
ID_SRV
ADD_SRV(= ADD_NET_X | ID_SRV)
150
(1) ダウンロードコマンド送信
(Sig(K_SEC_MBL
(Ticket_HS)),
K_PUB_HS−cert)
(2) Ticket_HS検証
(3) コンテンツのハッシュ値(H(M))計算
(7). 暗号化ハッシュ値を含むコンテンツパッケージ
[M | E(K_SEC2_MBL, H(M))]を生成
(4). H(M)
(5). 携帯情報端末の
秘密鍵(K_SEC2_MBL)で
H(M)暗号化
(6). E(K_SEC2_MBL, H(M))
(8).M | E(K_SEC2_MBL, H(M)
(9).K_PUB2_MBLで復号しH(M)を取り出す
H(M)の検証
120
ホームPC
ID_HS
ADD_HS(= ADD_NET_B | ID_HS)
130
携帯情報端末
ID_MBL
ADD_MBL(= ADD_NET_A | ID_MBL)

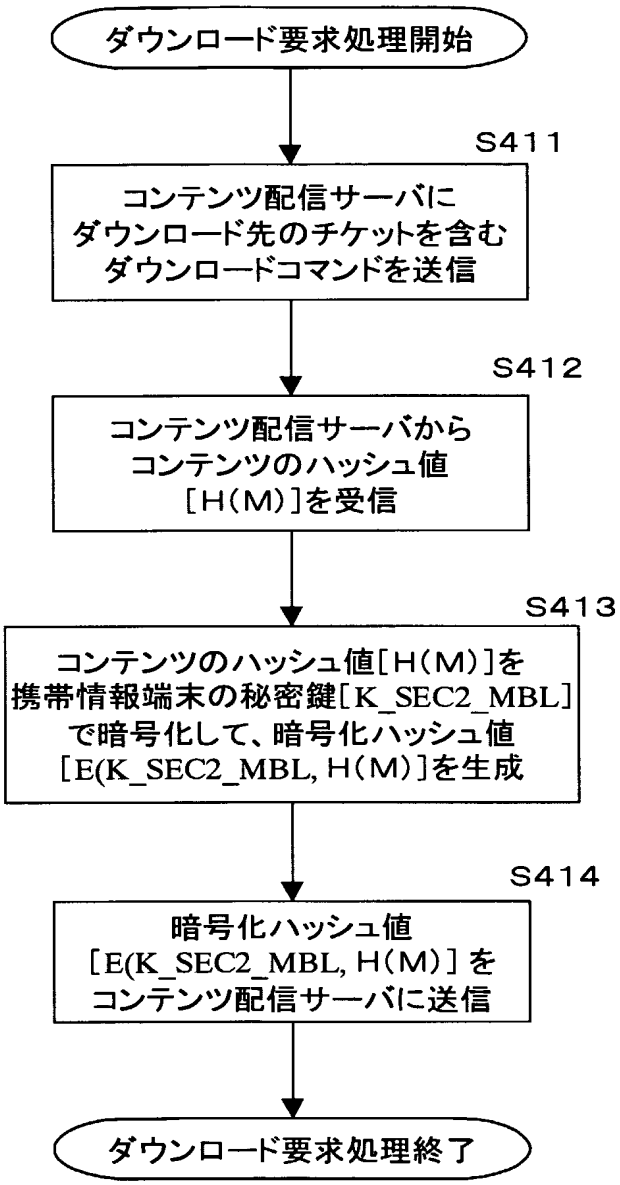

ダウンロード要求処理開始
S411
コンテンツ配信サーバに
ダウンロード先のチケットを含む
ダウンロードコマンドを送信
S412
コンテンツ配信サーバから
コンテンツのハッシュ値
[H(M)]を受信
S413
コンテンツのハッシュ値[H(M)]を
携帯情報端末の秘密鍵[K_SEC2_MBL]
で暗号化して、暗号化ハッシュ値
[E(K_SEC2_MBL, H(M)]を生成
S414
暗号化ハッシュ値
[E(K_SEC2_MBL, H(M)] を
コンテンツ配信サーバに送信
ダウンロード要求処理終了

Fig.16

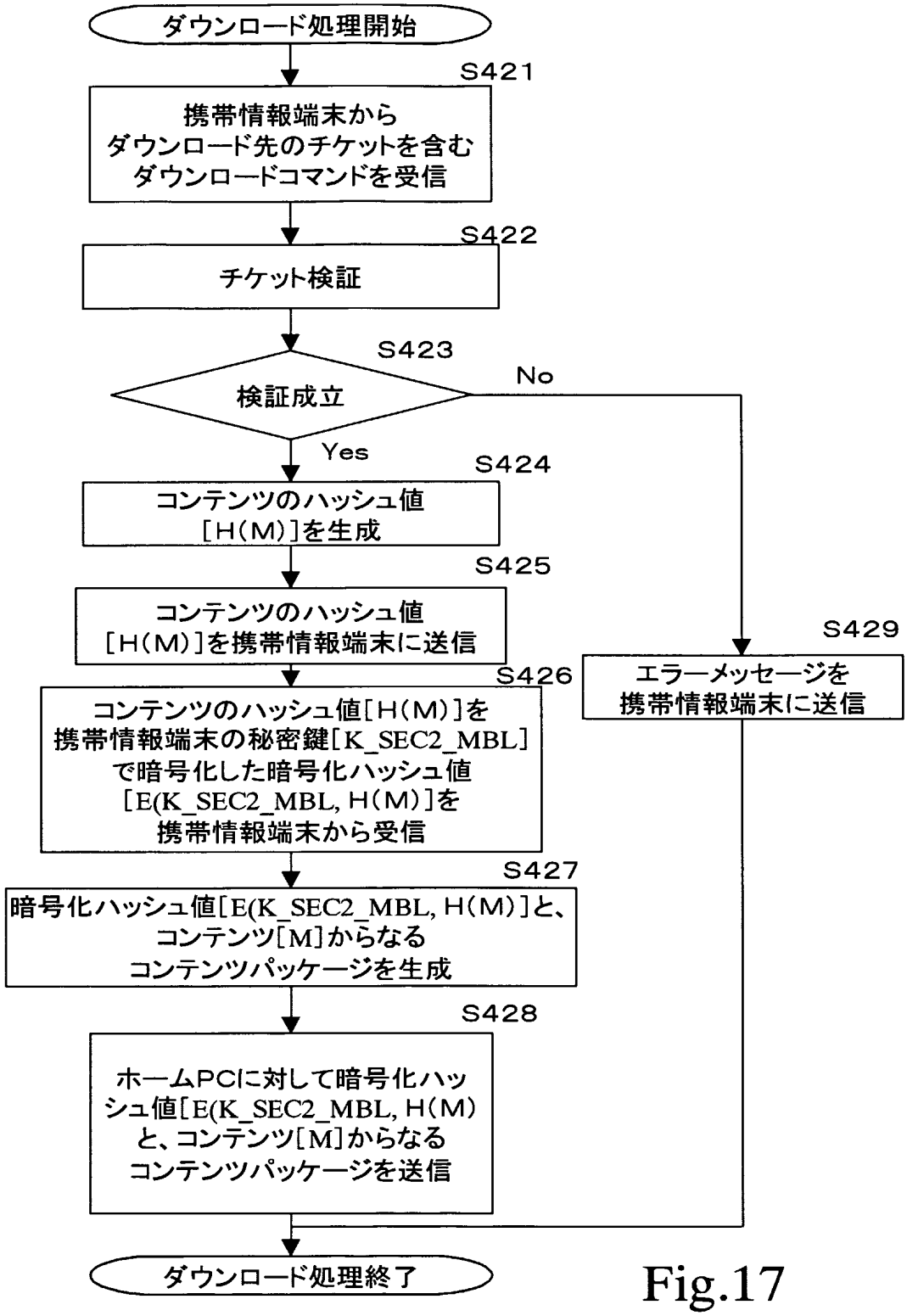

ダウンロード処理開始
S421
携帯情報端末から
ダウンロード先のチケットを含む
ダウンロードコマンドを受信
S422
チケット検証
S423
検証成立
No
Yes
S424
コンテンツのハッシュ値
[H(M)]を生成
S425
コンテンツのハッシュ値
[H(M)]を携帯情報端末に送信
S429
エラーメッセージを
携帯情報端末に送信
S426
コンテンツのハッシュ値[H(M)]を
携帯情報端末の秘密鍵[K_SEC2_MBL]
で暗号化した暗号化ハッシュ値
[E(K_SEC2_MBL, H(M)]を
携帯情報端末から受信
S427
暗号化ハッシュ値[E(K_SEC2_MBL, H(M)]と、
コンテンツ[M]からなる
コンテンツパッケージを生成
S428
ホームPCに対して暗号化ハッ
シュ値[E(K_SEC2_MBL, H(M)
と、コンテンツ[M]からなる
コンテンツパッケージを送信
ダウンロード処理終了

Fig.17

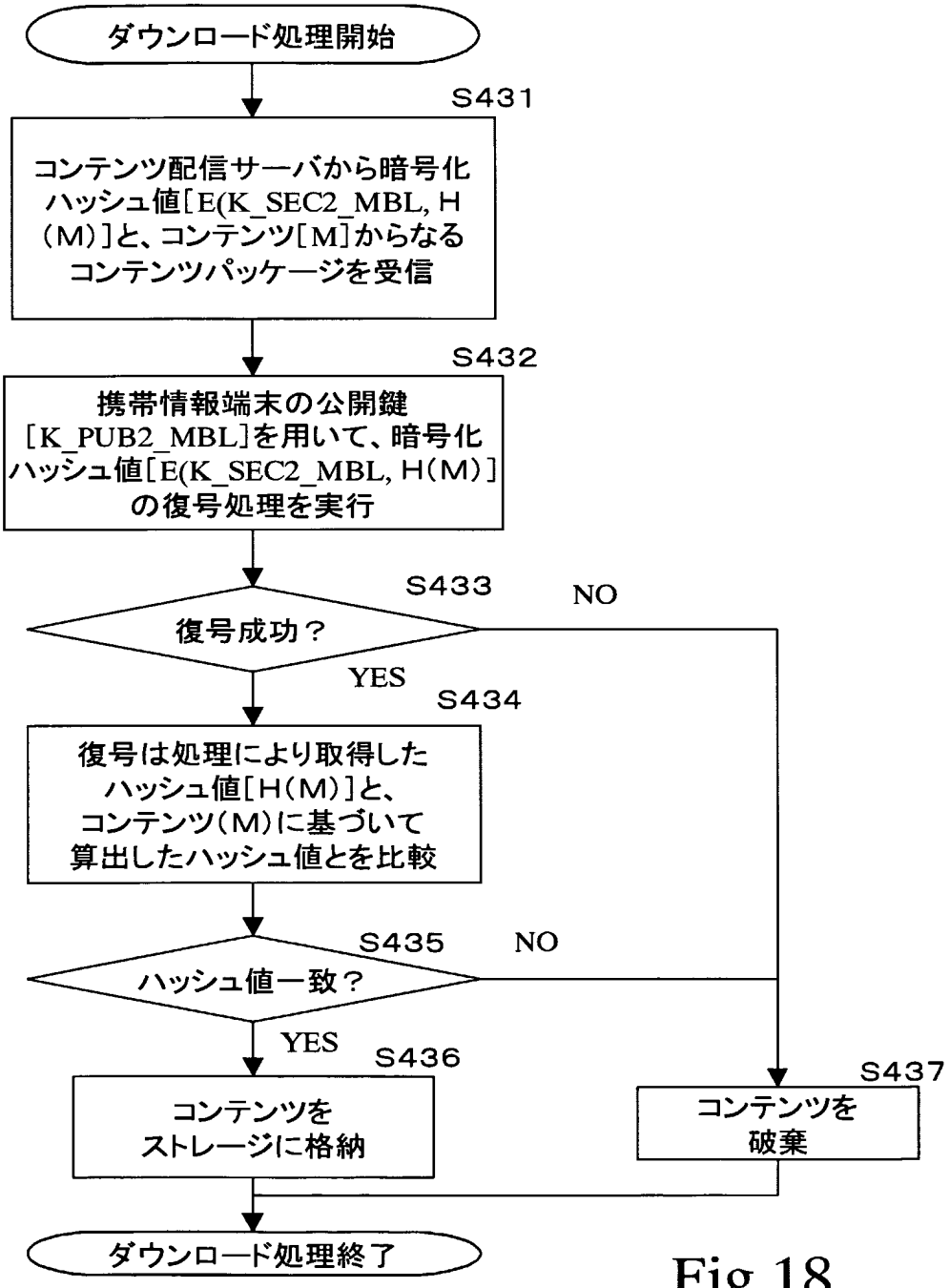
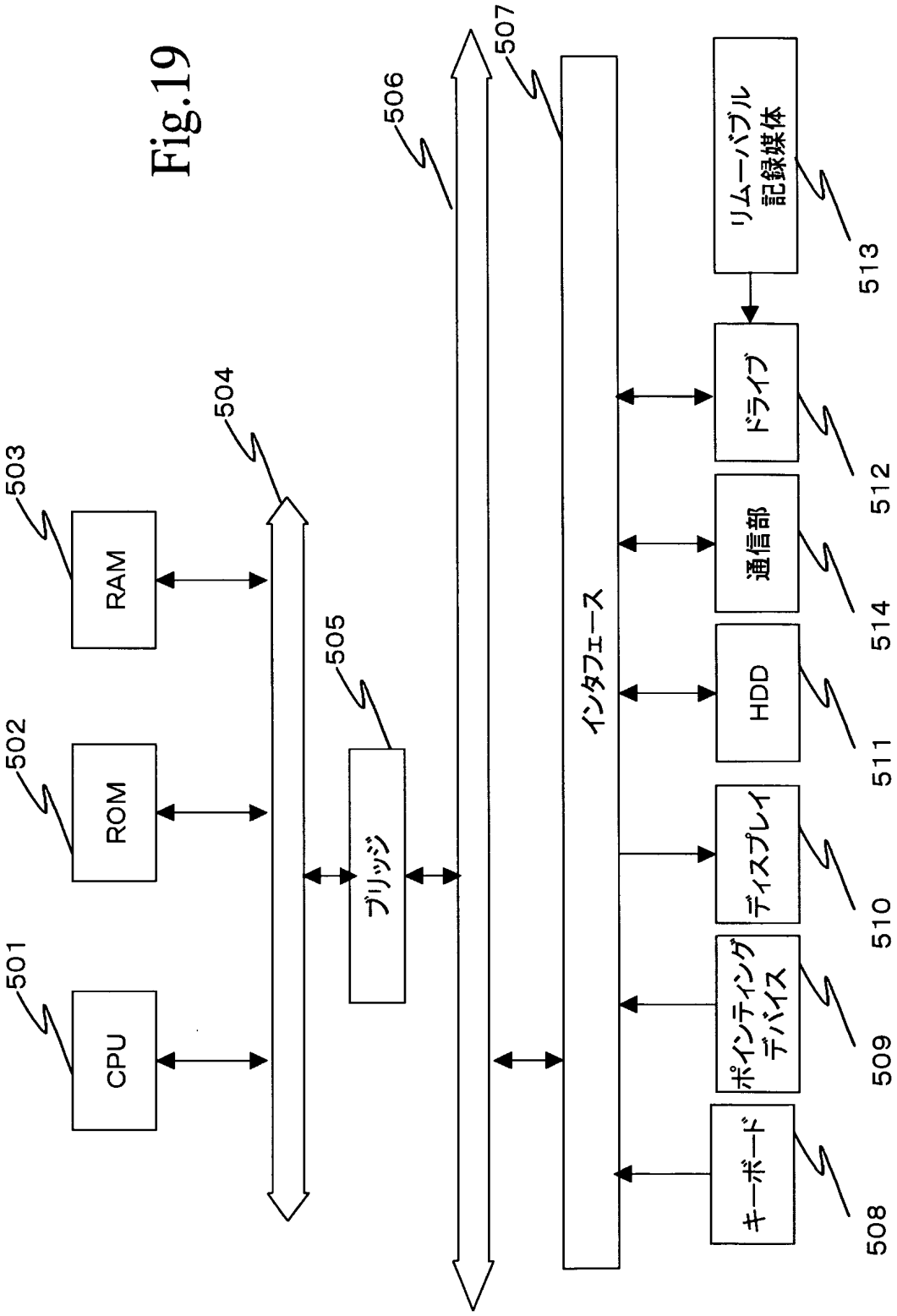

ダウンロード処理開始
S431
コンテンツ配信サーバから暗号化ハッシュ値[E(K_SEC2_MBL, H(M)]と、コンテンツ[M]からなるコンテンツパッケージを受信
S432
携帯情報端末の公開鍵[K_PUB2_MBL]を用いて、暗号化ハッシュ値[E(K_SEC2_MBL, H(M)]の復号処理を実行
S433
復号成功？
NO
YES
S434
復号は処理により取得したハッシュ値[H(M)]と、コンテンツ(M)に基づいて算出したハッシュ値とを比較
S435
ハッシュ値一致？
NO
YES
S436
コンテンツをストレージに格納
S437
コンテンツを破棄
ダウンロード処理終了

Fig.18

Fig.19


CPU
501
ROM
502
RAM
503
504
ブリッジ
505
506
507
インタフェース
キーボード
508
ポインティングデバイス
509
ディスプレイ
510
HDD
511
ドライブ
512
リムーバブル記録媒体
513
通信部
514

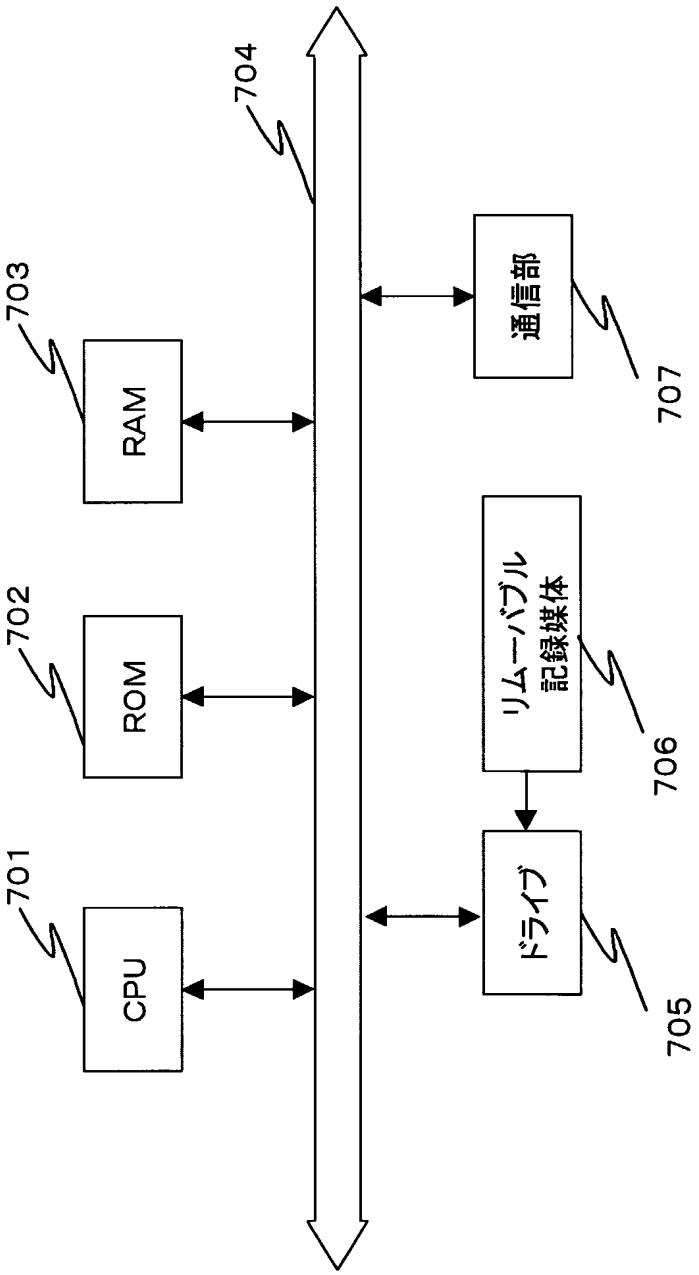


Fig.20

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/00107

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L9/32, G06F12/14, G06F15/00, G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L9/32, G06F12/14, G06F15/00, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 8-335208 A (Nippon Telegraph And Telephone Corp.), 17 December, 1996 (17.12.96), Full text; Figs. 1 to 21 (Family: none)	1-21
Y	JP 11-174956 A (International Business Machines Corp.), 02 July, 1999 (02.07.99), Par. Nos. [0009] to [0010], [0016] to [0021]; Figs. 1 to 3, 6 & US 6393563 B	1-21

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 07 April, 2003 (07.04.03)	Date of mailing of the international search report 22 April, 2003 (22.04.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/00107

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-285766 A (Matsushita Electric Industrial Co., Ltd.), 12 October, 2001 (12.10.01), Par. Nos. [0060] to [0063]; Fig. 1 (Family: none)	1-21
A	JP 2001-290912 A (NTT Data Corp.), 19 October, 2001 (19.10.01), Par. Nos. [0007], [0036] to [0040] (Family: none)	1-21
P,A	JP 2002-189908 A (Nippon Telegraph And Telephone Corp.), 05 July, 2002 (05.07.02), Full text; Figs. 1 to 30 (Family: none)	1-21

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／００１０７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／０８，Ｈ０４Ｌ９／３２，Ｇ０６Ｆ１２／１４，Ｇ０６Ｆ１５／００，Ｇ０６Ｆ１３／００

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／０８，Ｈ０４Ｌ９／３２，Ｇ０６Ｆ１２／１４，Ｇ０６Ｆ１５／００，Ｇ０６Ｆ１３／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００３年
日本国登録実用新案公報	１９９４－２００３年
日本国実用新案登録公報	１９９６－２００３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　８－３３５２０８　Ａ（日本電信電話株式会社） １９９６．１２．１７，全文，図１－２１ （ファミリーなし）	１－２１
Ｙ	ＪＰ　１１－１７４９５６　Ａ（インターナショナル・ビジネス・マシーンズ・コーポレイション） １９９９．０７．０２，第【０００９】－【００１０】段落，第【００１６】－【００２１】段落，図１－３，６ ＆　ＵＳ　６３９３５６３　Ｂ	１－２１

☒　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ０７．０４．０３	国際調査報告の発送日　22.04.03
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 青木　重徳　5M　4229 電話番号　０３－３５８１－１１０１　内線　３５９７

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／００１０７

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　２００１－２８５７６６　Ａ（松下電器産業株式会社） ２００１．１０．１２ 第【００６０】－【００６３】段落，図１ （ファミリーなし）	１－２１
Ａ	ＪＰ　２００１－２９０９１２　Ａ（株式会社エヌ・ティ・ティ・データ） ２００１．１０．１９， 第【０００７】段落，第【００３６】－【００４０】段落 （ファミリーなし）	１－２１
Ｐ，Ａ	ＪＰ　２００２－１８９９０８　Ａ（日本電信電話株式会社） ２００２．０７．０５，全文，図１－３０ （ファミリーなし）	１－２１